Titolo dell'opera originale
Introduction to Commutative Algebra

Traduzione dall'inglese di
Paolo Maroscia

Prima edizione italiana: gennaio 1981

M. F. Atiyah e *I. G. Macdonald*

Introduzione all'algebra commutativa

Appendice all'edizione italiana
di Paolo Maroscia

Feltrinelli Editore Milano

Indice

Avvertenza del traduttore

La versione italiana contiene alcune variazioni rispetto all'edizione originale inglese, le quali consistono per lo più, nella correzione di imprecisioni e, a volte, in lievi modifiche del testo.

Ringrazio con l'occasione gli Autori per avermi gentilmente comunicato un elenco aggiuntivo di "errata-corrige".

Prefazione

L'algebra commutativa è essenzialmente lo studio degli anelli commutativi. In breve, essa si è sviluppata da due fonti: (1) la geometria algebrica e (2) la teoria algebrica dei numeri. In (1) il prototipo degli anelli studiati è l'anello $k[x_1, \ldots, x_n]$ dei polinomi in più variabili sopra un campo k; in (2) è l'anello $\mathbf{Z}$ degli interi. Tra questi due, il caso algebro-geometrico è di gran lunga il più importante e, nel suo sviluppo moderno dovuto a Grothendieck, abbraccia molta parte della teoria algebrica dei numeri. L'algebra commutativa è attualmente uno dei fondamenti base di questa nuova geometria algebrica. Essa fornisce in maniera completa gli strumenti locali per tale studio, nello stesso modo in cui l'analisi differenziale fornisce gli strumenti per la geometria differenziale.

Questo libro è nato da un corso di lezioni impartite a studenti universitari del terzo anno presso l'Università di Oxford e si propone modestamente di fornire una rapida introduzione all'argomento. Esso è destinato agli studenti che hanno seguito un primo corso elementare di algebra generale. D'altra parte, questo libro non intende sostituirsi ai trattati più voluminosi di algebra commutativa quali Zariski-Samuel [4] o Bourbaki [1]. Ci siamo limitati ad approfondire alcuni argomenti centrali, mentre vasti capitoli, quali la teoria dei campi, non sono stati toccati. Nel contenuto vi è alquanto più materiale che in Northcott [3] e la nostra trattazione differisce essenzialmente per il fatto che, seguendo la tendenza moderna, diamo maggiore importanza ai moduli e alla localizzazione.

La nozione centrale in algebra commutativa è quella di ideale primo. Essa fornisce una generalizzazione sia dei primi dell'aritmetica, sia dei punti della geometria. La nozione geometrica dello studio "nell'intorno di un punto" ha come analogo algebrico l'importante processo di *localizzazione* di un anello in un ideale primo. Pertanto, non c'è da meravigliarsi che risultati relativi alla localizzazione possono essere riespressi utilmente in termini geometrici. Ciò viene fatto sistematicamente nella teoria degli *schemi* di Grothendieck e, in parte come introduzione all'opera di Grothendieck [2], in parte per la visione geometrica che essa fornisce, abbiamo aggiunto le versioni "schematiche" di molti risultati sotto forma di esercizi e osservazioni.

Il carattere originario di appunti di lezioni del libro spiega lo stile piuttosto conciso, con poche digressioni generali, e il carattere succinto di molte dimostrazioni. Abbiamo resistito alla tentazione di ampliare il libro con la speranza che la brevità della nostra presentazione avrebbe reso più chiara la struttura matematica di quella che è ormai una teoria elegante e di grande interesse. La nostra filosofia è stata quella di pervenire ai teoremi principali attraverso una successione di passaggi semplici, e di omettere verifiche ovvie.

Chiunque scriva oggi sull'algebra commutativa si trova di fronte a un dilemma riguardo all'algebra omologica, che svolge un ruolo cosí importante nei moderni sviluppi. Una trattazione appropriata dell'algebra omologica è impossibile entro i confini di un piccolo libro: d'altra parte, è alquanto difficile ignorarla completamente. Il compromesso che abbiamo adottato è stato quello di utilizzare i metodi omologici elementari (successioni esatte, diagrammi, ecc.), ma di fermarci subito davanti a qualsiasi risultato che richiede uno studio approfondito dell'omologia. In tal modo speriamo di preparare il terreno per un corso sistematico sull'algebra omologica che il lettore affronterà qualora desideri proseguire lo studio della geometria algebrica in profondità.

Abbiamo riportato un buon numero di esercizi alla fine di ogni capitolo. Alcuni di essi sono facili e altri sono impegnativi. Di solito abbiamo fornito suggerimenti, e talvolta soluzioni complete, per quelli piú difficili. Siamo molto grati a R. Y. Sharp, il quale ha lavorato su di essi evitandoci in piú occasioni di commettere errori.

Non abbiamo fatto alcun tentativo di descrivere i contributi dei numerosi matematici ai quali si deve lo sviluppo della teoria cosí come è stata esposta in questo libro. Tuttavia, siamo lieti di riconoscere il nostro debito verso J.-P. Serre e J. Tate dai quali abbiamo appreso la materia, e la cui influenza è stata determinante nella nostra scelta degli argomenti e nel modo di presentarli.

Bibliografia

1. N. Bourbaki, *Algèbre Commutative*, Hermann, Paris 1961-65.
2. A. Grothendieck e J. Dieudonné, *Eléments de Géometrie Algébri-*

que, Publications Mathématiques de l'I.H.E.S., nn. 4, 8, 11, Paris 1960 sgg.

3. D. G. NORTHCOTT, *Ideal Theory*, Cambridge University Press, 1953.
4. O. ZARISKI e P. SAMUEL, *Commutative Algebra* I, II, Van Nostrand, Princeton 1958, 1960.

Notazioni e terminologia

Gli anelli e i moduli sono denotati con lettere corsive maiuscole, i loro elementi con lettere corsive minuscole. Un campo viene indicato spesso con k. Gli ideali sono denotati con lettere gotiche minuscole. $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ indicano rispettivamente l'anello dei numeri interi, il campo dei numeri razionali, il campo dei numeri reali e il campo dei numeri complessi.

Le applicazioni sono scritte sempre sulla *sinistra*, sicché l'immagine di un elemento x in un'applicazione f si scrive $f(x)$ e non $(x)f$. La composizione di applicazioni $f\colon X \to Y$, $g\colon Y \to Z$ è pertanto $g \circ f$, non $f \circ g$.

Un'applicazione $f\colon X \to Y$ è *iniettiva* se $f(x_1) = f(x_2)$ implica $x_1 = x_2$; *suriettiva* se $f(X) = Y$; *biiettiva* se è simultaneamente iniettiva e suriettiva.

La fine di una dimostrazione (o l'assenza di dimostrazione) è indicata così ■.

L'inclusione di insiemi è denotata col simbolo $\subseteq$. La notazione $\subset$ indica esclusivamente inclusioni in senso *stretto*. Dunque $A \subset B$ significa che A è contenuto in B e non è uguale a B.

Capitolo primo

Anelli e ideali

Cominceremo con il passare in rassegna rapidamente la definizione e le proprietà elementari di un anello. Ciò servirà a indicare quanto supporremo noto al lettore e, inoltre, a fissare notazioni e convenzioni. Dopo tale rassegna, passiamo ad esaminare gli ideali primi e gli ideali massimali. Il resto del capitolo è dedicato all'illustrazione delle varie operazioni elementari che possono essere eseguite sugli ideali. Il linguaggio degli schemi, dovuto a Grothendieck, è introdotto negli esercizi, alla fine del capitolo.

Anelli e omomorfismi di anelli

Un *anello* A è un insieme con due operazioni binarie (addizione e moltiplicazione) tali che:

1) A è un gruppo abeliano rispetto all'addizione (sicché A possiede un elemento neutro, denotato con 0, e ogni elemento $x \in A$ ha un opposto, $-x$).

2) La moltiplicazione è associativa ($(xy)z = x(yz)$) e distributiva rispetto all'addizione ($x(y+z) = xy + xz$, $(y+z)x = yx + zx$).

Considereremo soltanto anelli che sono *commutativi*:

3) $xy = yx$, $\forall\, x, y \in A$,

e possiedono un *elemento unità* (denotato con 1):

4) $\exists 1 \in A$ tale che $x1 = 1x = x$, $\forall\, x \in A$.

L'elemento unità è allora unico.

D'ora in poi, il termine "anello" indicherà sempre un anello commutativo con unità, ossia un anello soddisfacente agli assiomi da (1) a (4) di cui sopra.

Osservazione. Non si esclude l'eventualità in (4) che 1 possa essere uguale a 0. In tal caso, per ogni elemento $x \in A$ si ha

$$x = x1 = x0 = 0$$

e quindi A possiede soltanto un elemento, 0. Allora A è l'*anello nullo*, denotato con 0 (per abuso di notazione).

Un *omomorfismo di anelli* è un'applicazione f di un anello A in un anello B tale che:

i) $f(x+y) = f(x) + f(y)$ (sicché f è un omomorfismo di gruppi abeliani, e pertanto si ha anche $f(x-y) = f(x) - f(y)$, $f(-x) = -f(x)$, $f(0) = 0$),

ii) $f(xy) = f(x)f(y)$,

iii) $f(1) = 1$.

In altre parole, f conserva l'addizione, la moltiplicazione e l'elemento unità.

Un sottoinsieme S di un anello A è un *subanello* (o *sottoanello*) di A, se S è un sottogruppo additivo di A tale che è chiuso rispetto alla moltiplicazione e contiene l'elemento unità di A. L'applicazione identica di S in A è allora un omomorfismo di anelli.

Se $f\colon A \to B$, $g\colon B \to C$ sono omomorfismi di anelli, allora tale è la loro composizione $g \circ f\colon A \to C$.

Ideali, anelli quozienti

Un *ideale* $\mathfrak{a}$ di un anello A è un sottoinsieme di A che è un sottogruppo additivo ed è tale che $A\mathfrak{a} \subseteq \mathfrak{a}$ (ossia, se $x \in A$ e $y \in \mathfrak{a}$, allora $xy \in \mathfrak{a}$). Il gruppo quoziente $A/\mathfrak{a}$ eredita una moltiplicazione definita in modo unico da A che lo rende un anello, chiamato l'*anello quoziente* (o anello delle classi resto) $A/\mathfrak{a}$. Gli elementi di $A/\mathfrak{a}$ sono le classi laterali di $\mathfrak{a}$ in A, e l'applicazione $\phi\colon A \to A/\mathfrak{a}$ che manda ogni elemento $x \in A$ nella classe laterale $x + \mathfrak{a}$ è un omomorfismo suriettivo di anelli.

Utilizzeremo spesso il risultato seguente:

Proposizione 1.1. *Esiste una corrispondenza biunivoca, che conserva l'ordinamento, tra gli ideali* $\mathfrak{b}$ *di* A *che contengono* $\mathfrak{a}$ *e gli ideali* $\bar{\mathfrak{b}}$ *di* $A/\mathfrak{a}$ *data da*: $\mathfrak{b} = \phi^{-1}(\bar{\mathfrak{b}})$. ■

Se $f\colon A \to B$ è un qualsiasi omomorfismo di anelli, il *nucleo* di $f(= f^{-1}(0))$ è un ideale $\mathfrak{a}$ di A, e l'*immagine* di $f(= f(A))$ è un subanello C di B; inoltre, f induce un isomorfismo di anelli $A/\mathfrak{a} \cong C$.

Talvolta useremo la notazione $x \equiv y \pmod{\mathfrak{a}}$; ciò significa che $x - y \in \mathfrak{a}$.

Divisori dello zero, elementi nilpotenti, elementi invertibili

Un *divisore dello zero* in un anello A è un elemento x che "divide 0", ossia per il quale esiste un elemento $y \neq 0$ in A tale che $xy = 0$. Un anello privo di divisori dello zero $\neq 0$ (e nel quale $1 \neq 0$) è chiamato un *dominio di integrità*. Per esempio, $\mathbf{Z}$ e $k[x_1, \ldots, x_n]$ (essendo k un campo e le x_i indeterminate) sono domini di integrità.

Un elemento $x \in A$ è *nilpotente* se $x^n = 0$ per qualche $n > 0$. Un elemento nilpotente è un divisore dello zero (a meno che $A = 0$), ma non viceversa (in generale).

Un elemento *invertibile* in A è un elemento x che "divide 1", ossia un elemento x tale che $xy = 1$, per qualche $y \in A$. L'elemento y è allora determinato univocamente da x, e si denota con x^{-1}. Gli elementi invertibili in A formano un gruppo abeliano (moltiplicativo).

I multipli ax di un elemento $x \in A$ formano un ideale *principale*, denotato con (x) oppure Ax. Un elemento x è invertibile $\Leftrightarrow (x) = A = (1)$. L'ideale *zero* (0) si denota di solito con 0.

Un *campo* è un anello A in cui $1 \neq 0$ ed ogni elemento non nullo è invertibile. Ogni campo è un dominio di integrità (ma non viceversa: $\mathbf{Z}$ non è un campo).

Proposizione 1.2. *Sia A un anello $\neq 0$. Allora le seguenti condizioni sono equivalenti:*

i) *A è un campo;*

ii) *gli unici ideali di A sono 0 e (1);*

iii) *ogni omomorfismo di A in un anello non nullo B è iniettivo.*

Dimostrazione. i) $\Rightarrow$ ii). Sia $\mathfrak{a} \neq 0$ un ideale di A. Allora $\mathfrak{a}$ contiene un elemento non nullo x; x è invertibile, dunque $\mathfrak{a} \supseteq (x) = (1)$, da cui $\mathfrak{a} = (1)$.

ii) $\Rightarrow$ iii). Sia $\phi\colon A \to B$ un omomorfismo di anelli. Allora $\operatorname{Ker}(\phi)$ è un ideale $\neq (1)$ in A, sicché $\operatorname{Ker}(\phi) = 0$, dunque ϕ è iniettivo.

iii) $\Rightarrow$ i). Sia x un elemento non invertibile di A. Allora $(x) \neq (1)$, dunque $B = A/(x)$ non è l'anello nullo. Sia $\phi\colon A \to B$ l'omomorfismo naturale di A su B, con nucleo (x). Per ipotesi, ϕ è iniettivo, dunque $(x) = 0$, da cui $x = 0$. ■

Ideali primi e ideali massimali

Un ideale $\mathfrak{p}$ di A è *primo*, se $\mathfrak{p} \neq (1)$ e se $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ oppure $y \in \mathfrak{p}$.

Un ideale $\mathfrak{m}$ di A è *massimale*, se $\mathfrak{m} \neq (1)$ e se non esiste alcun ideale $\mathfrak{a}$ tale che $\mathfrak{m} \subset \mathfrak{a} \subset (1)$ (inclusioni *strette*). In modo equivalente:

$\mathfrak{p}$ è primo $\Leftrightarrow A/\mathfrak{p}$ è un dominio di integrità;

$\mathfrak{m}$ è massimale $\Leftrightarrow A/\mathfrak{m}$ è un campo (cfr. (1.1) e (1.2)).

Dunque un ideale massimale è primo (ma non viceversa, in generale). L'ideale nullo è primo $\Leftrightarrow A$ è un dominio di integrità.

Se $f: A \rightarrow B$ è un omomorfismo di anelli e $\mathfrak{q}$ è un ideale primo di B, allora $f^{-1}(\mathfrak{q})$ è un ideale primo di A, poiché $A/f^{-1}(\mathfrak{q})$ è isomorfo ad un subanello di $B/\mathfrak{q}$ e quindi non possiede divisori dello zero $\neq 0$. Ma se $\mathfrak{n}$ è un ideale massimale di B, non è necessariamente vero che $f^{-1}(\mathfrak{n})$ è massimale in A; tutto ciò che si può dire è che esso è primo. (Esempio: $A = \mathbf{Z}$, $B = \mathbf{Q}$, $\mathfrak{n} = 0$).

Gli ideali primi sono fondamentali per l'intera algebra commutativa. Il teorema seguente ed i suoi corollari assicurano che ve n'è sempre una quantità sufficiente.

Teorema 1.3. *Ogni anello $A \neq 0$ possiede almeno un ideale massimale.* (Da ricordare che "anello" significa anello commutativo con unità.)

Dimostrazione. Si tratta di un'applicazione standard del lemma di Zorn.* Sia Σ l'insieme di tutti gli ideali $\neq (1)$ in A. Ordiniamo Σ rispetto all'inclusione. Σ è non vuoto, poiché $0 \in \Sigma$. Per applicare il lemma di Zorn, dobbiamo mostrare che ogni catena in Σ possiede un maggiorante in Σ; sia allora $(\mathfrak{a}_\alpha)$ una catena di ideali in Σ, cosicché per ogni coppia di indici α, β si ha $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\beta$ oppure $\mathfrak{a}_\beta \subseteq \mathfrak{a}_\alpha$. Sia $\mathfrak{a} = \bigcup_\alpha \mathfrak{a}_\alpha$. Allora $\mathfrak{a}$ è un ideale (verificare ciò) e $1 \notin \mathfrak{a}$ poiché $1 \notin \mathfrak{a}_\alpha$

* Sia S un insieme non vuoto parzialmente ordinato (ossia, è data una relazione $x < y$ su S, la quale è riflessiva e transitiva e tale che $x < y$ e $y < x$ insieme implicano $x = y$). Un sottoinsieme T di S è una *catena*, se $x < y$ oppure $y < x$ per ogni coppia di elementi x, y in T. Allora il lemma di Zorn può essere enunciato nel modo seguente: *se ogni catena T di S possiede un maggiorante in S* (ossia, se esiste un elemento $x \in S$ tale che $t < x$ per ogni $t \in T$), *allora S possiede almeno un elemento massimale.*

Per una dimostrazione dell'equivalenza del lemma di Zorn con l'assioma della scelta, il principio del buon ordinamento, ecc., cfr. per esempio P. R. Halmos, *Naive Set Theory*, Van Nostrand, 1960 (tr. it. *Teoria elementare degli insiemi*, Feltrinelli, Milano 1970).

per ogni α. Ne segue che $\mathfrak{a} \in \Sigma$, e $\mathfrak{a}$ è un maggiorante della catena. Dunque, in virtú del lemma di Zorn, Σ possiede un elemento massimale. ∎

Corollario 1.4. *Se $\mathfrak{a} \neq (1)$ è un ideale di A, allora esiste un ideale massimale di A che contiene $\mathfrak{a}$.*

Dimostrazione. Basta applicare (1.3) ad $A/\mathfrak{a}$, tenendo presente (1.1). Diversamente, basta modificare opportunamente la dimostrazione di (1.3). ∎

Corollario 1.5. *Ogni elemento non invertibile di A è contenuto in un ideale massimale.* ∎

Osservazioni. 1) Se A è noetheriano (Capitolo 7) si può evitare l'uso del lemma di Zorn: l'insieme di tutti gli ideali $\neq (1)$ possiede un elemento massimale.

2) Esistono anelli con un unico ideale massimale, per es. i campi. Un anello A con un unico ideale massimale $\mathfrak{m}$ è chiamato un *anello locale*. Il campo $k = A/\mathfrak{m}$ è chiamato il *campo residuo* di A.

Proposizione 1.6. i) *Sia A un anello e $\mathfrak{m} \neq (1)$ un ideale di A tale che ogni elemento $x \in A - \mathfrak{m}$ è invertibile in A. Allora A è un anello locale e $\mathfrak{m}$ è il suo ideale massimale.*

ii) *Sia A un anello e $\mathfrak{m}$ un ideale massimale di A, tale che ogni elemento di $1 + \mathfrak{m}$ (ossia, ogni elemento della forma $1 + x$, con $x \in \mathfrak{m}$) è invertibile in A. Allora A è un anello locale.*

Dimostrazione. i) Ogni ideale $\neq (1)$ è costituito da elementi non invertibili, quindi è contenuto in $\mathfrak{m}$. Dunque $\mathfrak{m}$ è l'unico ideale massimale di A.

ii) Sia $x \in A - \mathfrak{m}$. Poiché $\mathfrak{m}$ è massimale, l'ideale generato da x e $\mathfrak{m}$ è (1), sicché esistono elementi $y \in A$ e $t \in \mathfrak{m}$ tali che $xy + t = 1$; pertanto l'elemento $xy = 1 - t$ appartiene a $1 + \mathfrak{m}$ e quindi è invertibile. Ora basta usare i). ∎

Un anello che possiede soltanto un numero finito di ideali massimali è chiamato *semilocale*.

Esempi. 1) $A = k[x_1, \ldots, x_n]$, con k campo. Sia $f \in A$ un polinomio irriducibile. In virtú della fattorizzazione unica, l'ideale (f) è primo.

2) $A = \mathbf{Z}$. Ogni ideale in $\mathbf{Z}$ è della forma (m) per qualche $m \geq 0$. L'ideale (m) è primo $\Leftrightarrow m = 0$ oppure è un numero primo. Tutti gli

ideali (p), dove p è un numero primo, sono massimali: $\mathbf{Z}/(p)$ è il campo con p elementi.

Ciò vale anche nell'Esempio 1) per $n = 1$, ma non per $n > 1$. L'ideale $\mathfrak{m}$ di tutti i polinomi in $A = k[x_1, \ldots, x_n]$ con termine costante zero è massimale (poiché è il nucleo dell'omomorfismo $A \to k$ che manda $f \in A$ in $f(0)$). Ma, se $n > 1$, $\mathfrak{m}$ non è un ideale principale: infatti esso richiede almeno n generatori.

3) Un *dominio a ideali principali* è un dominio di integrità in cui ogni ideale è principale. In un anello siffatto ogni ideale primo non nullo è massimale. Infatti, se $(x) \neq 0$ è un ideale primo e $(y) \supset (x)$, si ha $x \in (y)$, diciamo $x = yz$, sicché $yz \in (x)$ e $y \notin (x)$, dunque $z \in (x)$: e sia $z = tx$. Allora $x = yz = ytx$, sicché $yt = 1$ e quindi $(y) = (1)$.

Il nilradicale e il radicale di Jacobson

Proposizione 1.7. *L'insieme $\mathfrak{N}$ di tutti gli elementi nilpotenti in un anello A è un ideale, e $A/\mathfrak{N}$ non possiede elementi nilpotenti $\neq 0$.*

Dimostrazione. Se $x \in \mathfrak{N}$, chiaramente $ax \in \mathfrak{N}$ per ogni $a \in A$. Siano $x, y \in \mathfrak{N}$: diciamo $x^m = 0$, $y^n = 0$. In virtù del teorema del binomio (che è valido in qualsiasi anello commutativo), $(x + y)^{m+n-1}$ è una somma di multipli interi di prodotti $x^r y^s$, dove $r + s = m + n - 1$; non si può avere simultaneamente $r < m$ e $s < n$, dunque ciascuno di tali prodotti si annulla e pertanto $(x + y)^{m+n-1} = 0$. Ne segue che $x + y \in \mathfrak{N}$ e quindi $\mathfrak{N}$ è un ideale.

Sia $\bar{x} \in A/\mathfrak{N}$ rappresentato da $x \in A$. Allora $\bar{x}^n$ è rappresentato da x^n, sicché $\bar{x}^n = 0 \Rightarrow x^n \in \mathfrak{N} \Rightarrow (x^n)^k = 0$ per qualche $k > 0 \Rightarrow x \in \mathfrak{N} \Rightarrow \bar{x} = 0$. ∎

L'ideale $\mathfrak{N}$ è chiamato il *nilradicale* di A. La seguente proposizione fornisce una definizione alternativa di $\mathfrak{N}$:

[illegible]

Proposizione 1.8. *Il nilradicale di A è l'intersezione di tutti gli ideali primi di A.*

Dimostrazione. Denotiamo con $\mathfrak{N}'$ l'intersezione di tutti gli ideali primi di A. Se $f \in A$ è nilpotente e se $\mathfrak{p}$ è un ideale primo, allora $f^n = 0 \in \mathfrak{p}$ per qualche $n > 0$, quindi $f \in \mathfrak{p}$ (poiché $\mathfrak{p}$ è primo). Dunque $f \in \mathfrak{N}'$.

Viceversa, supponiamo che f non sia nilpotente. Sia Σ l'insieme degli ideali $\mathfrak{a}$ con la proprietà

$$n > 0 \Rightarrow f^n \notin \mathfrak{a}.$$

Allora Σ è non vuoto, giacché $0 \in \Sigma$. Come in (1.3), il lemma di Zorn può venir applicato all'insieme Σ, ordinato rispetto all'inclusione, e pertanto Σ possiede un elemento massimale. Sia $\mathfrak{p}$ un elemento massimale di Σ. Mostreremo che $\mathfrak{p}$ è un ideale primo. Siano $x, y \notin \mathfrak{p}$. Allora gli ideali $\mathfrak{p} + (x)$, $\mathfrak{p} + (y)$ contengono strettamente $\mathfrak{p}$ e quindi non appartengono a Σ; pertanto

$$f^m \in \mathfrak{p} + (x), \; f^n \in \mathfrak{p} + (y)$$

con m, n interi opportuni. Ne segue che $f^{m+n} \in \mathfrak{p} + (xy)$, sicché l'ideale $\mathfrak{p} + (xy)$ non appartiene a Σ e pertanto $xy \notin \mathfrak{p}$. Dunque abbiamo un ideale primo $\mathfrak{p}$ tale che $f \notin \mathfrak{p}$, sicché $f \notin \mathfrak{N}'$. ■

Il *radicale di Jacobson* $\mathfrak{R}$ di A è definito come l'intersezione di tutti gli ideali massimali di A. Esso può essere caratterizzato nel modo seguente:

Proposizione 1.9. $x \in \mathfrak{R} \Leftrightarrow 1 - xy$ *è invertibile in* A *per ogni* $y \in A$.

Dimostrazione. $\Rightarrow$: Supponiamo che $1 - xy$ non sia invertibile. In virtú di (1.5) esso appartiene a qualche ideale massimale $\mathfrak{m}$; ma $x \in \mathfrak{R} \subseteq \mathfrak{m}$, dunque $xy \in \mathfrak{m}$ e pertanto $1 \in \mathfrak{m}$, ciò che è assurdo.

$\Leftarrow$: Supponiamo che $x \notin \mathfrak{m}$ per qualche ideale massimale $\mathfrak{m}$. Allora $\mathfrak{m}$ e x generano l'ideale unità (1), sicché si ha $u + xy = 1$ per qualche $u \in \mathfrak{m}$ e qualche $y \in A$. Ne segue che $1 - xy \in \mathfrak{m}$ e quindi non è invertibile. ■

Operazioni sugli ideali

Se $\mathfrak{a}$, $\mathfrak{b}$ sono ideali in un anello A, la loro *somma* $\mathfrak{a} + \mathfrak{b}$ è l'insieme di tutti gli elementi $x + y$, dove $x \in \mathfrak{a}$ e $y \in \mathfrak{b}$. Esso è il piú piccolo ideale contenente $\mathfrak{a}$ e $\mathfrak{b}$. Piú in generale, si può definire la somma $\sum_{i \in I} \mathfrak{a}_i$ di una qualsiasi famiglia (eventualmente infinita) di ideali $\mathfrak{a}_i$ di A; i suoi elementi sono tutte le somme $\sum x_i$, dove $x_i \in \mathfrak{a}_i$ per ogni $i \in I$ e quasi tutti gli x_i (ossia, tutti tranne un insieme finito) sono nulli. Esso è il piú piccolo ideale di A che contiene tutti gli ideali $\mathfrak{a}_i$.

L'*intersezione* di una qualsiasi famiglia $(\mathfrak{a}_i)_{i\in I}$ di ideali è un ideale. Dunque gli ideali di A formano un reticolo completo rispetto all'inclusione.

Il *prodotto* di due ideali $\mathfrak{a}, \mathfrak{b}$ in A è l'ideale $\mathfrak{ab}$ *generato* da tutti i prodotti xy, dove $x \in \mathfrak{a}$ e $y \in \mathfrak{b}$. Esso è l'insieme di tutte le somme finite $\sum x_i y_i$ dove ciascun $x_i \in \mathfrak{a}$ e ciascun $y_i \in \mathfrak{b}$. Allo stesso modo si definisce il prodotto di una qualsiasi famiglia *finita* di ideali. In particolare, vengono definite le potenze $\mathfrak{a}^n$ $(n > 0)$ di un ideale $\mathfrak{a}$; per convenzione, $\mathfrak{a}^0 = (1)$. Così $\mathfrak{a}^n$ $(n > 0)$ è l'ideale generato da tutti i prodotti $x_1 x_2 \ldots x_n$ in cui ciascun fattore x_i appartiene ad $\mathfrak{a}$.

Esempi. 1) Se $A = \mathbf{Z}$, $\mathfrak{a} = (m)$, $\mathfrak{b} = (n)$, allora $\mathfrak{a} + \mathfrak{b}$ è l'ideale generato dal M.C.D. di m e n; $\mathfrak{a} \cap \mathfrak{b}$ è l'ideale generato dal loro m.c.m.; e $\mathfrak{ab} = (mn)$. Dunque (in questo caso) $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b} \Leftrightarrow m, n$ sono coprimi.

2) $A = k[x_1, \ldots, x_n]$, $\mathfrak{a} = (x_1, \ldots, x_n) =$ ideale generato da $x_1, \ldots, x_n$. Allora $\mathfrak{a}^m$ è l'insieme di tutti i polinomi privi di termini di grado $< m$.

Le tre operazioni finora definite (somma, intersezione, prodotto) sono tutte commutative e associative. Vale anche la *legge distributiva*

$$\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{ab} + \mathfrak{ac}.$$

Nell'anello $\mathbf{Z}$, le operazioni $\cap$ e $+$ sono distributive l'una rispetto all'altra. Ciò non è vero in generale e il risultato migliore che si ha in proposito è la *legge modulare*

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}, \text{ se } \mathfrak{a} \supseteq \mathfrak{b} \text{ oppure } \mathfrak{a} \supseteq \mathfrak{c}.$$

Inoltre, in $\mathbf{Z}$, si ha $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{ab}$; ma in generale si ha soltanto $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{ab}$ (poiché $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{ab}$). Chiaramente $\mathfrak{ab} \subseteq \mathfrak{a} \cap \mathfrak{b}$, da cui

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}, \text{ purché } \mathfrak{a} + \mathfrak{b} = (1).$$

Due ideali $\mathfrak{a}, \mathfrak{b}$ si dicono *coprimi* (o comassimali), se $\mathfrak{a} + \mathfrak{b} = (1)$. Dunque per ideali coprimi si ha $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$. Chiaramente due ideali $\mathfrak{a}, \mathfrak{b}$ sono coprimi se, e soltanto se, esistono elementi $x \in \mathfrak{a}$ e $y \in \mathfrak{b}$ tali che $x + y = 1$.

Siano $A_1, \ldots, A_n$ anelli. Il loro *prodotto diretto*

$$A = \prod_{i=1}^{n} A_i$$

è l'insieme di tutte le n-ple $x = (x_1, \ldots, x_n)$ con $x_i \in A_i$ $(1 \leq i \leq n)$, in cui l'addizione e la moltiplicazione sono definite componente per componente. A è un anello commutativo con elemento unità $(1, 1, \ldots, 1)$. Si hanno le proiezioni $p_i \colon A \to A_i$ definite da $p_i(x) = x_i$; esse sono omomorfismi di anelli.

Sia A un anello e siano $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideali di A. Definiamo un omomorfismo

$$\phi \colon A \to \prod_{i=1}^{n} (A/\mathfrak{a}_i)$$

mediante la legge $\phi(x) = (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$.

Proposizione 1.10. i) *Se* $\mathfrak{a}_i, \mathfrak{a}_j$ *sono coprimi per* $i \neq j$, *allora* $\Pi \mathfrak{a}_i = \cap \mathfrak{a}_i$.

ii) ϕ *è suriettivo* $\Leftrightarrow \mathfrak{a}_i, \mathfrak{a}_j$ *sono coprimi per* $i \neq j$.

iii) ϕ *è iniettivo* $\Leftrightarrow \cap \mathfrak{a}_i = (0)$.

Dimostrazione. i) si prova per induzione su n. Il caso $n = 2$ è stato visto sopra. Supponiamo $n > 2$ e il risultato vero per $\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}$ e poniamo $\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i = \bigcap_{i=1}^{n-1} \mathfrak{a}_i$. Poiché $\mathfrak{a}_i + \mathfrak{a}_n = (1)$ $(1 \leq i \leq n-1)$ si hanno equazioni della forma $x_i + y_i = 1$ $(x_i \in \mathfrak{a}_i, y_i \in \mathfrak{a}_n)$ e pertanto

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{\mathfrak{a}_n}.$$

Ne segue che $\mathfrak{a}_n + \mathfrak{b} = (1)$ e quindi

$$\prod_{i=1}^{n} \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

ii) $\Rightarrow$: Mostriamo, per esempio, che $\mathfrak{a}_1, \mathfrak{a}_2$ sono coprimi. Allora esiste un elemento $x \in A$ tale che $\phi(x) = (1, 0, \ldots, 0)$; dunque $x \equiv 1 \pmod{\mathfrak{a}_1}$ e $x \equiv 0 \pmod{\mathfrak{a}_2}$, sicché

$$1 = (1 - x) + x \in \mathfrak{a}_1 + \mathfrak{a}_2.$$

$\Leftarrow$: È sufficiente mostrare, per esempio, che esiste un elemento $x \in A$ tale che $\phi(x) = (1, 0, \ldots, 0)$. Poiché $\mathfrak{a}_1 + \mathfrak{a}_i = (1)$ $(i > 1)$, si hanno equazioni della forma $u_i + v_i = 1$ $(u_i \in \mathfrak{a}_1, v_i \in \mathfrak{a}_i)$. Prendiamo $x = \prod_{i=2}^{n} v_i$, allora $x = \Pi(1 - u_i) \equiv 1 \pmod{\mathfrak{a}_1}$, e $x \equiv 0 \pmod{\mathfrak{a}_i}$, $i > 1$. Dunque $\phi(x) = (1, 0, \ldots, 0)$ come richiesto.

iii) si ottiene osservando che l'ideale $\bigcap \mathfrak{a}_i$ è il nucleo di ϕ. ∎

L'*unione* $\mathfrak{a} \cup \mathfrak{b}$ di ideali non è in generale un ideale.

Proposizione 1.11. i) *Siano* $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ *ideali primi e sia* $\mathfrak{a}$ *un ideale contenuto in* $\bigcup_{i=1}^{n} \mathfrak{p}_i$. *Allora* $\mathfrak{a} \subseteq \mathfrak{p}_i$ *per qualche* i.

ii) *Siano* $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *ideali e sia* $\mathfrak{p}$ *un ideale primo contenente* $\bigcap_{i=1}^{n} \mathfrak{a}_i$. *Allora* $\mathfrak{p} \supseteq \mathfrak{a}_i$ *per qualche* i. *Se* $\mathfrak{p} = \bigcap \mathfrak{a}_i$, *allora* $\mathfrak{p} = \mathfrak{a}_i$ *per qualche* i.

Dimostrazione. i) si prova per induzione su n nella forma

$$\mathfrak{a} \nsubseteq \mathfrak{p}_i \, (1 \leqslant i \leqslant n) \Rightarrow \mathfrak{a} \nsubseteq \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

Ciò è certamente vero per $n = 1$. Se $n > 1$ e il risultato è vero per $n - 1$, allora per ciascun indice i esiste un elemento $x_i \in \mathfrak{a}$ tale che $x_i \notin \mathfrak{p}_j$, per $j \neq i$. Se per qualche i si ha $x_i \notin \mathfrak{p}_i$, non c'è più nulla da dire. Altrimenti, si ha: $x_i \in \mathfrak{p}_i$ per ogni i. Consideriamo l'elemento

$$y = \sum_{i=1}^{n} x_1 x_2 \quad x_{i-1} x_{i+1} x_{i+2} \quad x_n;$$

si ha $y \in \mathfrak{a}$ e $y \notin \mathfrak{p}_i \, (1 \leqslant i \leqslant n)$. Dunque $\mathfrak{a} \nsubseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$.

ii) Supponiamo che $\mathfrak{p} \nsupseteq \mathfrak{a}_i$ per ogni i. Allora esistono elementi $x_i \in \mathfrak{a}_i$, $x_i \notin \mathfrak{p} \, (1 \leqslant i \leqslant n)$ e pertanto $\Pi x_i \in \Pi \mathfrak{a}_i \subseteq \bigcap \mathfrak{a}_i$; ma $\Pi x_i \notin \mathfrak{p}$ (poiché $\mathfrak{p}$ è primo). Dunque $\mathfrak{p} \nsupseteq \bigcap \mathfrak{a}_i$. Infine, se $\mathfrak{p} = \bigcap \mathfrak{a}_i$, allora $\mathfrak{p} \subseteq \mathfrak{a}_i$ e quindi $\mathfrak{p} = \mathfrak{a}_i$ per qualche i. ∎

Se $\mathfrak{a}, \mathfrak{b}$ sono ideali in un anello A, il loro *ideale quoziente* è

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A : x\mathfrak{b} \subseteq \mathfrak{a}\}$$

che è un ideale. In particolare, $(0 : \mathfrak{b})$ è chiamato l'*annullatore* di $\mathfrak{b}$ ed è anche denotato con $\mathrm{Ann}(\mathfrak{b})$: esso è l'insieme di tutti gli elementi $x \in A$ tali che $x\mathfrak{b} = 0$. Con questa notazione, l'insieme di tutti i divisori dello zero in A è

$$D = \bigcup_{x \neq 0} \mathrm{Ann}(x).$$

Se $\mathfrak{b}$ è un ideale principale (x), scriveremo $(\mathfrak{a} : x)$ in luogo di $(\mathfrak{a} : (x))$.

Esempio. Se $A = \mathbf{Z}$, $\mathfrak{a} = (m)$, $\mathfrak{b} = (n)$, dove, diciamo, $m = \prod_p p^{\mu_p}$, $n = \prod_p p^{\nu_p}$, allora $(\mathfrak{a} : \mathfrak{b}) = (q)$, dove $q = \prod_p p^{\gamma_p}$ e

$$\gamma_p = \max(\mu_p - \nu_p, 0) = \mu_p - \min(\mu_p, \nu_p).$$

Dunque $q = m/(m, n)$, dove (m, n) è il M.C.D. di m e n.

Esercizio 1.12. i) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$

ii) $(\mathfrak{a} : \mathfrak{b})\,\mathfrak{b} \subseteq \mathfrak{a}$

iii) $((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$

iv) $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$

v) $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$.

Se $\mathfrak{a}$ è un ideale qualsiasi di A, il *radicale* di $\mathfrak{a}$ è

$$r(\mathfrak{a}) = \{x \in A : x^n \in \mathfrak{a} \text{ per qualche } n > 0\}.$$

Se $\phi : A \to A/\mathfrak{a}$ è l'omomorfismo canonico, allora $r(\mathfrak{a}) = \phi^{-1}(\mathfrak{N}_{A/\mathfrak{a}})$ e quindi $r(\mathfrak{a})$ è un ideale, in virtú di (1.7).

Esercizio 1.13. i) $r(\mathfrak{a}) \supseteq \mathfrak{a}$

ii) $r(r(\mathfrak{a})) = r(\mathfrak{a})$

iii) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$

iv) $r(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a} = (1)$

v) $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$

vi) *se* $\mathfrak{p}$ *è primo,* $r(\mathfrak{p}^n) = \mathfrak{p}$ *per ogni* $n > 0$.

Proposizione 1.14. *Il radicale di un ideale* $\mathfrak{a}$ *è l'intersezione degli ideali primi che contengono* $\mathfrak{a}$.

Dimostrazione. Basta applicare (1.8) ad $A/\mathfrak{a}$. ■

Piú in generale, si può definire il radicale $r(E)$ di un *sottoinsieme* qualsiasi E di A nello stesso modo. Esso *non* è un ideale in generale. Si ha: $r(\bigcup_\alpha E_\alpha) = \bigcup_\alpha r(E_\alpha)$, per una qualsiasi famiglia di sottoinsiemi E_α di A.

Proposizione 1.15. $D =$ *insieme dei divisori dello zero di* $A = \bigcup_{x \neq 0} r(\operatorname{Ann}(x))$.

Dimostrazione. $D = r(D) = r(\bigcup_{x \neq 0} \operatorname{Ann}(x)) = \bigcup_{x \neq 0} r(\operatorname{Ann}(x))$. ■

Esempio. Se $A = \mathbf{Z}$, $\mathfrak{a} = (m)$, siano p_i $(1 \leqslant i \leqslant r)$ i divisori primi distinti di m. Allora $r(\mathfrak{a}) = (p_1 \ldots p_r) = \bigcap_{i=1}^{r} (p_i)$.

Proposizione 1.16. *Siano* $\mathfrak{a}, \mathfrak{b}$ *ideali in un anello* A *tali che* $r(\mathfrak{a}), r(\mathfrak{b})$ *sono coprimi. Allora* $\mathfrak{a}, \mathfrak{b}$ *sono coprimi.*

Dimostrazione. $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b})) = r(1) = (1)$, dunque $\mathfrak{a} + \mathfrak{b} = (1)$ in virtú di (1.13). ∎

Estensione e contrazione

Sia $f: A \to B$ un omomorfismo di anelli. Se $\mathfrak{a}$ è un ideale in A, l'insieme $f(\mathfrak{a})$ non è necessariamente un ideale in B (per es., sia f l'immersione di $\mathbf{Z}$ in $\mathbf{Q}$, il campo dei razionali, e sia $\mathfrak{a}$ un qualsiasi ideale non nullo in $\mathbf{Z}$). Si definisce l'*estensione* $\mathfrak{a}^e$ di $\mathfrak{a}$ come l'ideale $Bf(\mathfrak{a})$ generato da $f(\mathfrak{a})$ in B: esplicitamente, $\mathfrak{a}^e$ è l'insieme di tutte le somme del tipo $\sum y_i f(x_i)$ dove $x_i \in \mathfrak{a}, y_i \in B$.

Se $\mathfrak{b}$ è un ideale di B, allora $f^{-1}(\mathfrak{b})$ è sempre un ideale di A ed è chiamato la *contrazione* $\mathfrak{b}^c$ di $\mathfrak{b}$. Se $\mathfrak{b}$ è primo, allora $\mathfrak{b}^c$ è primo. Se $\mathfrak{a}$ è primo, $\mathfrak{a}^e$ non è necessariamente primo (per es., $f: \mathbf{Z} \to \mathbf{Q}, \mathfrak{a} \neq 0$; allora $\mathfrak{a}^e = \mathbf{Q}$, che non è un ideale primo).

Possiamo fattorizzare f nel modo seguente:

$$A \xrightarrow{p} f(A) \xrightarrow{j} B$$

dove p è suriettivo e j è iniettivo. Per p la situazione è molto semplice (1.1): vi è una corrispondenza biunivoca tra gli ideali di $f(A)$ e gli ideali di A che contengono $\operatorname{Ker}(f)$, e ideali primi corrispondono a ideali primi. Per j, d'altra parte, la situazione generale è molto complicata. L'esempio classico proviene dalla teoria algebrica dei numeri.

Esempio. Consideriamo $\mathbf{Z} \to \mathbf{Z}[i]$, dove $i = \sqrt{-1}$. Un ideale primo (p) di $\mathbf{Z}$ può o non restare primo quando viene esteso a $\mathbf{Z}[i]$. Infatti $\mathbf{Z}[i]$ è un dominio a ideali principali (poiché possiede un algoritmo euclideo) e la situazione è la seguente:

i) $(2)^e = ((1 + i)^2)$, il *quadrato* di un ideale primo in $\mathbf{Z}[i]$;

ii) se $p \equiv 1 \pmod 4$ allora $(p)^e$ è il prodotto di due ideali primi distinti (per es., $(5)^e = (2 + i)(2 - i)$);

iii) se $p \equiv 3 \pmod 4$ allora $(p)^e$ è primo in $\mathbf{Z}[i]$.

Tra tali risultati, ii) non è banale. Esso infatti è equivalente ad un teorema di Fermat il quale afferma che un primo $p \equiv 1 \pmod 4$ può venir espresso, essenzialmente in modo unico, come una somma di due quadrati interi (cosí $5 = 2^2 + 1^2$, $97 = 9^2 + 4^2$, ecc.).

In realtà il comportamento degli ideali primi rispetto ad estensioni di questo tipo è uno dei problemi centrali della teoria algebrica dei numeri.

Siano $f\colon A \to B$, $\mathfrak{a}$ e $\mathfrak{b}$ come sopra. Allora:

Proposizione 1.17. i) $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$, $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$;

ii) $\mathfrak{b}^c = \mathfrak{b}^{cec}$, $\mathfrak{a}^e = \mathfrak{a}^{ece}$;

iii) *Se C è l'insieme degli ideali contratti in A e se E è l'insieme degli ideali estesi in B, allora $C = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}$, $E = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$ e $\mathfrak{a} \mapsto \mathfrak{a}^e$ è una applicazione biiettiva di C su E, la cui inversa è $\mathfrak{b} \mapsto \mathfrak{b}^c$.*

Dimostrazione. i) è banale, e ii) segue da i).

iii) Se $\mathfrak{a} \in C$, allora $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{b}^{cec} = \mathfrak{a}^{ec}$; viceversa, se $\mathfrak{a} = \mathfrak{a}^{ec}$ allora $\mathfrak{a}$ è la contrazione di $\mathfrak{a}^e$. Similmente per E. ■

Esercizio 1.18. *Se $\mathfrak{a}_1, \mathfrak{a}_2$ sono ideali di A e se $\mathfrak{b}_1, \mathfrak{b}_2$ sono ideali di B, allora*

$$
\begin{array}{ll}
(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e, & (\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c, \\
(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e, & (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c, \\
(\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e, & (\mathfrak{b}_1\mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c\mathfrak{b}_2^c, \\
(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e), & (\mathfrak{b}_1 : \mathfrak{b}_2)^c \subseteq (\mathfrak{b}_1^c : \mathfrak{b}_2^c), \\
r(\mathfrak{a})^e \subseteq r(\mathfrak{a}^e), & r(\mathfrak{b})^c = r(\mathfrak{b}^c).
\end{array}
$$

L'insieme di ideali E è chiuso rispetto alla somma e al prodotto, e C è chiuso rispetto alle altre tre operazioni.

Esercizi

1. Sia x un elemento nilpotente di un anello A. Provare che $1 + x$ è invertibile in A. Dedurre che la somma di un elemento nilpotente e di un elemento invertibile è invertibile.

2. Sia A un anello e sia $A[x]$ l'anello dei polinomi in una indeterminata x, a coefficienti in A. Sia $f = a_0 + a_1x + \quad + a_nx^n \in A[x]$. Dimostrare che:

   i) f è invertibile in $A[x] \Leftrightarrow a_0$ è invertibile in A e $a_1, \dots, a_n$ sono nilpotenti. [Se $b_0 + b_1x + \dots + b_mx^m$ è l'inverso di f, provare per induzione su r che $a_n^{r+1}b_{m-r} = 0$. Dedurre da ciò che a_n è nilpotente, e quindi utilizzare l'Es. 1.]

   ii) f è nilpotente $\Leftrightarrow a_0, a_1, \dots, a_n$ sono nilpotenti.

iii) f è un divisore dello zero $\Leftrightarrow$ esiste un elemento $a \neq 0$ in A tale che $af = 0$. [Si scelga un polinomio $g = b_0 + b_1 x + + \quad + b_m x^m$ di grado minimo m tale che $fg = 0$. Allora $a_n b_m = 0$, da cui $a_n g = 0$ (poiché $a_n g$ annulla f ed ha grado $< m$). Ora provare per induzione che $a_{n-r} g = 0$ $(0 \leqslant r \leqslant n)$.]

iv) f si dice *primitivo* se $(a_0, a_1, \ldots, a_n) = (1)$. Provare che se $f, g \in A[x]$, allora fg è primitivo $\Leftrightarrow f$ e g sono primitivi.

3. Generalizzare i risultati dell'Esercizio 2 ad un anello di polinomi $A[x_1, \ldots, x_r]$ in piú indeterminate.

4. Nell'anello $A[x]$, il radicale di Jacobson è uguale al nilradicale.

5. Sia A un anello e sia $A[[x]]$ l'anello delle serie di potenze formali $f = \sum_{n=0}^{\infty} a_n x^n$ a coefficienti in A. Provare che:

   i) f è invertibile in $A[[x]] \Leftrightarrow a_0$ è invertibile in A.

   ii) Se f è nilpotente, allora a_n è nilpotente per ogni $n \geqslant 0$. È vero il viceversa? (Cfr. Capitolo 7, Esercizio 2)

   iii) f appartiene al radicale di Jacobson di $A[[x]] \Leftrightarrow a_0$ appartiene al radicale di Jacobson di A.

   iv) La contrazione di un ideale massimale $\mathfrak{m}$ di $A[[x]]$ è un ideale massimale di A, e $\mathfrak{m}$ è generato da $\mathfrak{m}^c$ e x.

   v) Ogni ideale primo di A è la contrazione di un ideale primo di $A[[x]]$.

6. Sia A un anello tale che ogni ideale non contenuto nel nilradicale contiene un elemento idempotente non nullo (ossia, un elemento e tale che $e^2 = e \neq 0$). Provare che il nilradicale e il radicale di Jacobson sono uguali.

7. Sia A un anello in cui ogni elemento x soddisfa ad una relazione della forma $x^n = x$ per qualche $n > 1$ (dipendente da x). Dimostrare che ogni ideale primo in A è massimale.

8. Sia A un anello $\neq 0$. Provare che l'insieme degli ideali primi di A possiede elementi minimali rispetto all'inclusione.

9. Sia $\mathfrak{a}$ un ideale $\neq (1)$ in un anello A. Provare che $\mathfrak{a} = r(\mathfrak{a}) \Leftrightarrow \mathfrak{a}$ è un'intersezione di ideali primi.

10. Sia A un anello, $\mathfrak{N}$ il suo nilradicale. Dimostrare che le seguenti proprietà sono equivalenti:

    i) A possiede un unico ideale primo;

    ii) ogni elemento di A è invertibile oppure è nilpotente;

    iii) $A/\mathfrak{N}$ è un campo.

11. Un anello A si dice *booleano*, se $x^2 = x$ per ogni $x \in A$. Provare che in un anello booleano A:
    i) $2x = 0$ per ogni $x \in A$;
    ii) ogni ideale primo $\mathfrak{p}$ è massimale, e $A/\mathfrak{p}$ è un campo con due elementi;
    iii) ogni ideale finitamente generato di A è principale.

12. Un anello locale non contiene elementi idempotenti $\neq 0, 1$.

Costruzione di una chiusura algebrica di un campo (E. Artin)

13. Sia K un campo e sia Σ l'insieme di tutti i polinomi monici irriducibili f in una indeterminata a coefficienti in K. Sia A l'anello dei polinomi sopra K generato dalle indeterminate x_f, una per ciascun $f \in \Sigma$. Sia $\mathfrak{a}$ l'ideale di A generato dai polinomi $f(x_f)$ per ogni $f \in \Sigma$. Provare che $\mathfrak{a} \neq (1)$.

    Sia $\mathfrak{m}$ un ideale massimale di A contenente $\mathfrak{a}$, e poniamo $K_1 = A/\mathfrak{m}$. Allora K_1 è un'estensione di K in cui ogni $f \in \Sigma$ possiede una radice. Ripetiamo la costruzione con K_1 al posto di K, ottenendo un campo K_2, e così via. Poniamo $L = \bigcup_{n=1}^{\infty} K_n$. Allora L è un campo in cui ogni $f \in \Sigma$ si spezza completamente in fattori lineari. Sia $\bar{K}$ l'insieme di tutti gli elementi di L che sono algebrici sopra K. Allora $\bar{K}$ è una chiusura algebrica di K.

14. In un anello A, sia Σ l'insieme di tutti gli ideali in cui ogni elemento è un divisore dello zero. Provare che l'insieme Σ possiede elementi massimali e che ogni elemento massimale di Σ è un ideale primo. Ne segue che l'insieme dei divisori dello zero in A è un'unione di ideali primi.

Lo spettro primo di un anello

15. Sia A un anello e sia X l'insieme di tutti gli ideali primi di A. Per ogni sottoinsieme E di A, denotiamo con $V(E)$ l'insieme di tutti gli ideali primi di A che contengono E. Dimostrare che:
    i) se $\mathfrak{a}$ è l'ideale generato da E, allora $V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$.
    ii) $V(0) = X$, $V(1) = \emptyset$.
    iii) se $(E_i)_{i \in I}$ è una qualsiasi famiglia di sottoinsiemi di A, allora

$$V(\bigcup_{i \in I} E_i) = \bigcap_{i \in I} V(E_i).$$

iv) $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{ab}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$, essendo $\mathfrak{a}, \mathfrak{b}$ ideali arbitrari di A.

Tali risultati mostrano che gli insiemi $V(E)$ soddisfano gli assiomi per i chiusi in uno spazio topologico. La topologia così ottenuta è chiamata la *topologia di Zariski*. Lo spazio topologico X è chiamato lo *spettro primo* di A, e si denota con Spec (A).

16. Fornire una descrizione grafica di Spec $(\mathbf{Z})$, Spec $(\mathbf{R})$, Spec $(\mathbf{C}[x])$, Spec $(\mathbf{R}[x])$, Spec $(\mathbf{Z}[x])$.

17. Per ogni elemento $f \in A$, denotiamo con X_f il complementare di $V(f)$ in $X =$ Spec (A). Gli insiemi X_f sono aperti. Dimostrare che essi formano una base di aperti per la topologia di Zariski, e che:
   i) $X_f \cap X_g = X_{fg}$;
   ii) $X_f = \varnothing \Leftrightarrow f$ è nilpotente;
   iii) $X_f = X \Leftrightarrow f$ è invertibile;
   iv) $X_f = X_g \Leftrightarrow r((f)) = r((g))$;
   v) X è quasi-compatto (ossia, ogni ricoprimento aperto di X possiede un sottoricoprimento finito);
   vi) piú in generale, ogni insieme X_f è quasi-compatto;
   vii) un aperto di X è quasi-compatto se, e soltanto se, è un'unione finita di insiemi X_f.

   Gli insiemi X_f sono chiamati *aperti fondamentali* di $X =$ Spec (A).

   [Per provare (v), osserviamo che basta considerare un ricoprimento di X costituito da aperti fondamentali $X_{f_i} (i \in I)$. Mostrare che gli elementi f_i generano l'ideale unità e quindi che si ha un'equazione della forma

$$1 = \sum_{i \in J} g_i f_i \qquad (g_i \in A)$$

   dove J è un opportuno sottoinsieme *finito* di I. Allora gli aperti $X_{f_i} (i \in J)$ ricoprono X.]

18. Per ragioni psicologiche, conviene talvolta denotare un ideale primo di A con una lettera quale x o y, quando esso viene pensato come un punto di $X =$ Spec (A). Quando si pensa ad x come un ideale primo di A, lo denotiamo con $\mathfrak{p}_x$ (naturalmente, da un punto di vista logico, è la stessa cosa). Dimostrare che:
   i) l'insieme $\{x\}$ è chiuso (si dice che x è un "punto chiuso") in Spec $(A) \Leftrightarrow \mathfrak{p}_x$ è massimale;

ii) $\overline{\{x\}} = V(\mathfrak{p}_x)$;

iii) $y \in \overline{\{x\}} \Leftrightarrow \mathfrak{p}_x \subseteq \mathfrak{p}_y$;

iv) X è uno spazio T_0 (ciò significa che se x, y sono punti distinti di X, allora esiste un intorno di x che non contiene y, oppure esiste un intorno di y che non contiene x).

19. Uno spazio topologico si dice *irriducibile*, se $X \neq \emptyset$ e se ogni coppia di aperti non vuoti di X si incontrano, o in modo equivalente, se ogni aperto non vuoto è denso in X. Provare che Spec(A) è irriducibile se, e soltanto se, il nilradicale di A è un ideale primo.

20. Sia X uno spazio topologico.

i) Se Y è un sottospazio irriducibile (Esercizio 19) di X, allora la chiusura $\bar{Y}$ di Y in X è irriducibile.

ii) Ogni sottospazio irriducibile di X è contenuto in un sottospazio irriducibile massimale.

iii) I sottospazi irriducibili massimali di X sono chiusi e ricoprono X. Essi prendono il nome di *componenti irriducibili* di X. Quali sono le componenti irriducibili di uno spazio di Hausdorff?

iv) Se A è un anello e $X = \text{Spec}(A)$, allora le componenti irriducibili di X sono i chiusi $V(\mathfrak{p})$, dove $\mathfrak{p}$ è un ideale primo minimale di A (Esercizio 8).

21. Sia $\phi: A \to B$ un omomorfismo di anelli. Poniamo $X = \text{Spec}(A)$ e $Y = \text{Spec}(B)$. Se $\mathfrak{q} \in Y$, allora $\phi^{-1}(\mathfrak{q})$ è un ideale primo di A, ossia, un punto di X. Dunque ϕ induce un'applicazione $\phi^*: Y \to X$. Dimostrare che:

i) Se $f \in A$, allora $\phi^{*-1}(X_f) = Y_{\phi(f)}$, e quindi che ϕ^* è continua.

ii) Se $\mathfrak{a}$ è un ideale di A, allora $\phi^{*-1}(V(\mathfrak{a})) = V(\mathfrak{a}^e)$.

iii) Se $\mathfrak{b}$ è un ideale di B, allora $\overline{\phi^*(V(\mathfrak{b}))} = V(\mathfrak{b}^c)$.

iv) Se ϕ è suriettivo, allora ϕ^* è un omeomorfismo di Y sul chiuso $V(\text{Ker}(\phi))$ di X. (In particolare, Spec(A) e Spec$(A/\mathfrak{N})$ (dove $\mathfrak{N}$ è il nilradicale di A) sono omeomorfi, in modo naturale.)

v) Se ϕ è iniettivo, allora $\phi^*(Y)$ è denso in X. Più precisamente, $\phi^*(Y)$ è denso in $X \Leftrightarrow \text{Ker}(\phi) \subseteq \mathfrak{N}$.

vi) Sia $\psi: B \to C$ un altro omomorfismo di anelli. Allora $(\psi \circ \phi)^* = \phi^* \circ \psi^*$.

vii) Sia A un dominio di integrità con un unico ideale primo non nullo $\mathfrak{p}$, e sia K il campo delle frazioni di A. Sia $B = (A/\mathfrak{p}) \times$ $\times K$. Definiamo $\phi: A \to B$ ponendo $\phi(x) = (\bar{x}, x)$, dove $\bar{x}$ è l'immagine di x in $A/\mathfrak{p}$. Provare che ϕ^* è biiettivo ma non è un omeomorfismo.

22. Sia $A = \prod_{i=1}^{n} A_i$ il prodotto diretto degli anelli A_i. Dimostrare che Spec(A) è l'unione disgiunta dei sottospazi aperti (e chiusi) X_i, dove X_i è canonicamente omeomorfo a Spec(A_i).

    Viceversa, sia A un anello. Provare che le seguenti condizioni sono equivalenti:

    i) $X = \text{Spec}(A)$ è sconnesso.
    ii) $A \cong A_1 \times A_2$ dove nessuno degli anelli A_1, A_2 è l'anello nullo.
    iii) A contiene un elemento idempotente $\neq 0, 1$.

    In particolare, lo spettro di un anello locale è sempre connesso (Esercizio 12).

23. Sia A un anello booleano (Esercizio 11), e sia $X = \text{Spec}(A)$.
    i) Per ogni $f \in A$, l'insieme X_f (Esercizio 17) è aperto e chiuso in X.
    ii) Siano $f_1, \dots, f_n \in A$. Provare che $X_{f_1} \cup \quad \cup X_{f_n} = X_f$ per qualche $f \in A$.
    iii) Gli insiemi X_f sono gli unici sottoinsiemi di X che sono simultaneamente aperti e chiusi.
    [Sia $Y \subseteq X$ un sottoinsieme simultaneamente aperto e chiuso. Poiché Y è aperto, esso è un'unione di aperti fondamentali X_f. Poiché Y è chiuso e X è quasi-compatto (Esercizio 17), Y è quasi-compatto. Dunque Y è un'unione finita di aperti fondamentali; a questo punto, basta utilizzare la (ii) di cui sopra.]
    iv) X è uno spazio di Hausdorff compatto.

24. Sia L un reticolo, in cui il sup e l'inf di due elementi a, b sono denotati, rispettivamente, con $a \vee b$ e $a \wedge b$. L è un *reticolo booleano* (o un'*algebra booleana*) se
    i) L possiede un minimo e un massimo (denotati rispettivamente con 0, 1).
    ii) Ciascuna delle operazioni $\vee$, $\wedge$ è distributiva rispetto all'altra.
    iii) Ogni elemento $a \in L$ possiede un unico "complemento" $a' \in L$ tale che $a \vee a' = 1$ e $a \wedge a' = 0$.

(Per esempio, l'insieme di tutti i sottoinsiemi di un insieme, ordinato rispetto all'inclusione, è un reticolo booleano).

Sia L un reticolo booleano. Definiamo l'addizione e la moltiplicazione in L mediante le regole

$$a + b = (a \wedge b') \vee (a' \wedge b), \qquad ab = a \wedge b.$$

Verificare che in questo modo L diventa un anello booleano, diciamo $A(L)$.

Viceversa, partendo da un anello booleano A, definiamo un ordinamento su A nel modo seguente: $a \leqslant b$ significa che $a = ab$. Provare che, rispetto a tale ordinamento, A è un reticolo booleano. [Il sup e l'inf sono dati da $a \vee b = a + b + ab$ e $a \wedge b = ab$, e il complemento da $a' = 1 - a$.] In tal modo si ottiene una corrispondenza biunivoca tra (le classi di isomorfismo di) anelli booleani e (le classi di isomorfismo di) reticoli booleani.

Dedurre dagli ultimi due esercizi il teorema di Stone, secondo cui "ogni reticolo booleano è isomorfo al reticolo dei sottoinsiemi simultaneamente aperti e chiusi di qualche spazio topologico di Hausdorff compatto".

Sia A un anello. Il sottospazio di Spec(A) costituito dagli ideali *massimali* di A, con la topologia indotta, è chiamato lo *spettro massimale* di A e si denota con Max(A). Per anelli commutativi arbitrari esso non ha le buone proprietà funtoriali di Spec(A) (cfr. Esercizio 21), poiché la controimmagine di un ideale massimale in un omomorfismo di anelli può non essere massimale.

Sia X uno spazio di Hausdorff compatto e denotiamo con $C(X)$ l'anello di tutte le funzioni a valori reali continue su X (le funzioni vengono sommate e moltiplicate, sommando e moltiplicando i loro valori). Per ogni $x \in X$, sia $\mathfrak{m}_x$ l'insieme di tutte le funzioni $f \in C(X)$ tali che $f(x) = 0$. L'ideale $\mathfrak{m}_x$ è massimale, poiché è il nucleo dell'omomorfismo (suriettivo) $C(X) \to \mathbf{R}$ che porta f in $f(x)$. Se $\tilde{X}$ denota Max$(C(X))$, resta così definita un'applicazione $\mu: X \to \tilde{X}$, precisamente $x \mapsto \mathfrak{m}_x$.

Proveremo che μ è un omeomorfismo di X su $\tilde{X}$.

i) Sia $\mathfrak{m}$ un ideale massimale arbitrario di $C(X)$, e sia $V = V(\mathfrak{m})$ l'insieme degli zeri comuni delle funzioni in $\mathfrak{m}$: ossia,

$$V = \{x \in X : f(x) = 0 \text{ per ogni } f \in \mathfrak{m}\}.$$

Supponiamo che V sia vuoto. Allora per ogni $x \in X$ esiste una funzione $f_x \in \mathfrak{m}$ tale che $f_x(x) \neq 0$. Poiché f_x è continua, esiste un intorno aperto U_x di x in X sul quale f_x non si annulla. Per ragioni di compattezza, un numero finito di tali intorni, diciamo $U_{x_1}, \ldots, U_{x_n}$, ricopre X. Poniamo

$$f = f_{x_1}^2 + \quad + f_{x_n}^2.$$

Allora f non si annulla in nessun punto di X, sicché è invertibile in $C(X)$. Ma ciò contraddice la relazione $f \in \mathfrak{m}$, dunque V è non vuoto.

Sia x un punto di V. Allora $\mathfrak{m} \subseteq \mathfrak{m}_x$, da cui $\mathfrak{m} = \mathfrak{m}_x$ poiché $\mathfrak{m}$ è massimale. Dunque μ è suriettivo.

ii) In virtú del lemma di Urysohn (questo è l'unico fatto non banale richiesto nella dimostrazione), le funzioni continue separano i punti di X. Dunque $x \neq y \Rightarrow \mathfrak{m}_x \neq \mathfrak{m}_y$, e pertanto μ è iniettivo.

iii) Sia $f \in C(X)$; poniamo

$$U_f = \{x \in X : f(x) \neq 0\}$$

e poniamo

$$\tilde{U}_f = \{\mathfrak{m} \in \tilde{X} : f \notin \mathfrak{m}\}.$$

Provare che $\mu(U_f) = \tilde{U}_f$. Gli aperti U_f (risp. $\tilde{U}_f$) formano una base della topologia di X (risp. $\tilde{X}$) e pertanto μ è un omeomorfismo.

In tal modo X può essere ricostruito a partire dall'anello di funzioni $C(X)$.

Varietà algebriche affini

27. Sia k un campo algebricamente chiuso e sia

$$f_\alpha(t_1, \ldots, t_n) = 0$$

un insieme di equazioni polinomiali in n variabili a coefficienti in k. L'insieme X di tutti i punti $x = (x_1, \quad, x_n) \in k^n$ che soddisfano a tali equazioni è una *varietà algebrica affine*.

Consideriamo l'insieme di tutti i polinomi $g \in k[t_1, \ldots, t_n]$ con la proprietà che $g(x) = 0$ per ogni $x \in X$. Tale insieme è un ideale $I(X)$ nell'anello dei polinomi, ed è chiamato l'*ideale della varietà* X. L'anello quoziente

$$P(X) = k[t_1, \ldots, t_n]/I(X)$$

è l'anello delle funzioni polinomiali su X, poiché due polinomi g, h definiscono la medesima funzione polinomiale su X se, e soltanto se, $g - h$ si annulla in ogni punto di X, ossia, se e soltanto se $g - h \in I(X)$.

Sia ξ_i l'immagine di t_i in $P(X)$. Le $\xi_i (1 \leqslant i \leqslant n)$ sono le *funzioni coordinate* su X: se $x \in X$, allora $\xi_i(x)$ è l'i-esima coordinata di x. $P(X)$ è generato come k-algebra dalle funzioni coordinate, ed è chiamato l'*anello delle coordinate* (o l'algebra affine) di X.

Come nell'Esercizio 26, per ogni $x \in X$ sia $\mathfrak{m}_x$ l'ideale di tutte le funzioni $f \in P(X)$ tali che $f(x) = 0$; esso è un ideale massimale di $P(X)$. Dunque, se $\tilde{X} = \operatorname{Max}(P(X))$, resta definita un'applicazione $\mu: X \to \tilde{X}$, precisamente $x \mapsto \mathfrak{m}_x$.

È facile provare che μ è iniettiva: se $x \neq y$, si deve avere $x_i \neq y_i$ per qualche i $(1 \leqslant i \leqslant n)$, e quindi $\xi_i - x_i$ appartiene a $\mathfrak{m}_x$ ma non a $\mathfrak{m}_y$, sicché $\mathfrak{m}_x \neq \mathfrak{m}_y$. Ciò che è meno banale (ma pur vero) è che μ è *suriettiva*. Si tratta di una delle forme del Teorema degli zeri di Hilbert (cfr. Capitolo 7).

28. Siano $f_1, \ldots, f_m$ elementi di $k[t_1, \ldots, t_n]$. Essi individuano un'*applicazione polinomiale* $\phi: k^n \to k^m$: se $x \in k^n$, le coordinate di $\phi(x)$ sono $f_1(x), \ldots, f_m(x)$.

    Siano X, Y varietà algebriche affini in k^n, k^m rispettivamente. Un'applicazione $\phi: X \to Y$ si dice *regolare*, se ϕ è la restrizione a X di un'applicazione polinomiale da k^n a k^m.

    Se η è una funzione polinomiale su Y, allora $\eta \circ \phi$ è una funzione polinomiale su X. Dunque ϕ induce un omomorfismo di k-algebre $P(Y) \to P(X)$, precisamente $\eta \mapsto \eta \circ \phi$. Provare che in tal modo si ottiene una corrispondenza biunivoca tra le applicazioni regolari $X \to Y$ e gli omomorfismi di k-algebre $P(Y) \to P(X)$.

Capitolo secondo

Moduli

Uno dei caratteri che contraddistinguono l'approccio moderno all'Algebra commutativa è la maggiore importanza data ai moduli, piuttosto che agli ideali. Ciò consente di procedere con maggiore chiarezza e semplicità. Per esempio, un ideale $\mathfrak{a}$ e il suo anello quoziente $A/\mathfrak{a}$ sono entrambi esempi di moduli e quindi, fino ad un certo punto, possono venir trattati su uno stesso piano. In questo capitolo diamo la definizione e le proprietà elementari dei moduli. Diamo anche una breve trattazione dei prodotti tensoriali, che contiene una discussione del loro comportamento rispetto alle successioni esatte.

Moduli e omomorfismi di moduli

Sia A un anello (commutativo, come sempre). Un *A-modulo* è un gruppo abeliano M (scritto additivamente) su cui A agisce linearmente: piú precisamente, è una coppia (M, μ), dove M è un gruppo abeliano e μ è un'applicazione di $A \times M$ in M tale che, se scriviamo ax per indicare $\mu(a, x)(a \in A, x \in M)$, i seguenti assiomi sono soddisfatti:

$$\begin{aligned} a(x+y) &= ax + ay, \\ (a+b)x &= ax + bx, \\ (ab)x &= a(bx), \\ 1x &= x \qquad\qquad (a, b \in A;\ x, y \in M). \end{aligned}$$

(In modo equivalente, M è un gruppo abeliano insieme con un omomorfismo di anelli $A \rightarrow E(M)$, dove $E(M)$ è l'anello degli endomorfismi del gruppo abeliano M.)

La nozione di A-modulo è una generalizzazione comune di parecchie nozioni familiari, come mostrano i seguenti esempi:

Esempi. 1) Un ideale $\mathfrak{a}$ di A è un A-modulo. In particolare, A stesso è un A-modulo.

2) Se A è un campo k, allora A-modulo $=$ k-spazio vettoriale.

3) $A = \mathbf{Z}$, allora $\mathbf{Z}$-modulo $=$ gruppo abeliano (definendo nx come $x + \ldots + x$).

4) $A = k[x]$, dove k è un campo; un A-modulo è un k-spazio vettoriale insieme con una trasformazione lineare.

5) $G =$ gruppo finito, $A = k[G] =$ algebra-gruppo di G sul campo k (sicché A non è commutativo, a meno che G non lo sia). Allora A-modulo $=$ k-rappresentazione di G.

Siano M, N A-moduli. Un'applicazione $f\colon M \to N$ è un *omomorfismo di A-moduli* (ossia, è *A-lineare*) se

$$f(x+y) = f(x) + f(y)$$
$$f(ax) = a \cdot f(x)$$

per ogni elemento $a \in A$ e per ogni coppia di elementi $x, y \in M$. Dunque f è un omomorfismo di gruppi abeliani che commuta rispetto all'azione di ciascun elemento $a \in A$. Se A è un campo, un omomorfismo di A-moduli è la stessa cosa che una trasformazione lineare di spazi vettoriali.

La composizione di omomorfismi di A-moduli è ancora un omomorfismo di A-moduli.

L'insieme di tutti gli omomorfismi di A-moduli da M a N può venir dotato di una struttura di A-modulo nel modo seguente: definiamo $f + g$ e af mediante le regole

$$(f+g)(x) = f(x) + g(x),$$
$$(af)(x) = a \cdot f(x)$$

per ogni $x \in M$. È banale verificare che gli assiomi di un A-modulo sono soddisfatti. Tale A-modulo si denota con $\mathrm{Hom}_A(M, N)$ (o anche $\mathrm{Hom}(M, N)$ se non vi è alcuna ambiguità riguardo all'anello A).

Omomorfismi del tipo $u\colon M' \to M$ e $v\colon N \to N''$ inducono delle applicazioni

$$\bar{u}\colon \mathrm{Hom}(M, N) \to \mathrm{Hom}(M', N) \quad \text{e} \quad \bar{v}\colon \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'')$$

definite nel modo seguente:

$$\bar{u}(f) = f \circ u, \quad \bar{v}(f) = v \circ f.$$

Tali applicazioni sono omomorfismi di A-moduli.

Per un qualsiasi modulo M si ha un isomorfismo naturale $\mathrm{Hom}(A, M) \cong M$: ogni omomorfismo di A-moduli $f: A \to M$ è univocamente determinato da $f(1)$, che può essere un arbitrario elemento di M.

Sottomoduli e moduli quozienti

Un *sottomodulo* M' di M è un sottogruppo di M che è chiuso rispetto alla moltiplicazione per gli elementi di A. Il gruppo abeliano M/M' allora eredita una struttura di A-modulo da M, definita ponendo $a(x + M') = ax + M'$ L'A-modulo M/M' è il *quoziente* di M rispetto a M'. L'applicazione naturale di M su M/M' è un omomorfismo di A-moduli. Vi è una corrispondenza biunivoca che conserva l'ordinamento tra i sottomoduli di M che contengono M' e i sottomoduli di M/M' (esattamente come per gli ideali; il risultato per gli ideali è un caso speciale).

Se $f: M \to N$ è un omomorfismo di A-moduli, il *nucleo* di f è l'insieme

$$\mathrm{Ker}(f) = \{x \in M : f(x) = 0\}$$

ed è un sottomodulo di M. L'*immagine* di f è l'insieme

$$\mathrm{Im}(f) = f(M)$$

ed è un sottomodulo di N. Il *conucleo* di f è

$$\mathrm{Coker}(f) = N/\mathrm{Im}(f)$$

che è un modulo quoziente di N.

Se M' è un sottomodulo di M tale che $M' \subseteq \mathrm{Ker}(f)$, allora f dà origine ad un omomorfismo $\bar{f}: M/M' \to N$, definito nel modo seguente: se $\bar{x} \in M/M'$ è l'immagine di $x \in M$, allora $\bar{f}(\bar{x}) = f(x)$. Il nucleo di $\bar{f}$ è $\mathrm{Ker}(f)/M'$. L'omomorfismo $\bar{f}$ è detto *indotto* da f. In particolare, prendendo $M' = \mathrm{Ker}(f)$, si ha un isomorfismo di A-moduli

$$M/\mathrm{Ker}(f) \cong \mathrm{Im}(f).$$

Operazioni sui sottomoduli

La maggior parte delle operazioni sugli ideali considerate nel primo capitolo hanno il loro corrispettivo per i moduli. Sia M un A-modulo e sia $(M_i)_{i \in I}$ una famiglia di sottomoduli di M. La loro *somma*

$\sum M_i$ è l'insieme di tutte le somme (finite) $\sum x_i$, dove $x_i \in M_i$ per ogni $i \in I$, e quasi tutti gli x_i (ossia, tutti tranne un numero finito) sono zero. $\sum M_i$ è il piú piccolo sottomodulo di M che contiene tutti gli M_i.

L'intersezione $\bigcap M_i$ è ancora un sottomodulo di M. Dunque i sottomoduli di M formano un reticolo completo rispetto all'inclusione.

Proposizione 2.1. i) *Se $L \supseteq M \supseteq N$ sono A-moduli, allora*

$$(L/N)/(M/N) \cong L/M.$$

ii) *Se M_1, M_2 sono sottomoduli di M, allora*

$$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2).$$

Dimostrazione. i) Si definisce un'applicazione $\theta\colon L/N \to L/M$ ponendo $\theta(x + N) = x + M$. Allora θ è un omomorfismo di A-moduli ben definito di L/N su L/M, e il suo nucleo è M/N, da cui (i).

ii) L'omomorfismo composto $M_2 \to M_1 + M_2 \to (M_1 + M_2)/M_1$ è suriettivo, e il suo nucleo è $M_1 \cap M_2$, da cui (ii). ∎

In generale non si può definire il *prodotto* di due sottomoduli, ma si può definire il prodotto $\mathfrak{a}M$, dove $\mathfrak{a}$ è un ideale e M un A-modulo; esso è l'insieme di tutte le somme finite $\sum a_i x_i$ con $a_i \in \mathfrak{a}$, $x_i \in M$, ed è un sottomodulo di M.

Se N, P sono sottomoduli di M, si definisce $(N:P)$ come l'insieme di tutti gli elementi $a \in A$ tali che $aP \subseteq N$; esso è un *ideale* di A. In particolare, $(0:M)$ è l'insieme di tutti gli elementi $a \in A$ tali che $aM = 0$; tale ideale è chiamato l'*annullatore* di M e si denota anche con $\operatorname{Ann}(M)$. Se $\mathfrak{a} \subseteq \operatorname{Ann}(M)$, si può considerare M come un $A/\mathfrak{a}$-modulo, nel modo seguente: se $\bar{x} \in A/\mathfrak{a}$ è rappresentato da $x \in A$, si definisce $\bar{x}m = xm$ ($m \in M$): ciò è indipendente dalla scelta del rappresentante x di $\bar{x}$, poiché $\mathfrak{a}M = 0$.

Un A-modulo è *fedele* se $\operatorname{Ann}(M) = 0$. Se $\operatorname{Ann}(M) = \mathfrak{a}$, allora M è fedele come $A/\mathfrak{a}$-modulo.

Esercizio 2.2. i) $\operatorname{Ann}(M + N) = \operatorname{Ann}(M) \cap \operatorname{Ann}(N)$.

ii) $(N: P) = \operatorname{Ann}((N + P)/N)$.

Se x è un elemento di M, l'insieme di tutti i multipli ax ($a \in A$) è un sottomodulo di M, denotato con Ax oppure (x). Se $M = \sum_{i \in I} Ax_i$, si dice che gli elementi x_i formano un *sistema di generatori* di M; ciò significa che ogni elemento di M può venire espresso (non necessariamente in modo unico) come una combinazione lineare finita degli x_i a coefficienti in A. Un A-modulo M si dice *finitamente generato* se possiede un sistema finito di generatori.

Somma diretta e prodotto diretto

Se M, N sono A-moduli, la loro *somma diretta* $M \oplus N$ è l'insieme di tutte le coppie (x, y) con $x \in M$, $y \in N$. Esso è un A-modulo se definiamo l'addizione e la moltiplicazione per uno scalare nel modo ovvio:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$a(x, y) = (ax, ay).$$

Piú in generale, se $(M_i)_{i \in I}$ è una qualsiasi famiglia di A-moduli, si può definire la loro *somma diretta* $\bigoplus_{i \in I} M_i$; i suoi elementi sono le famiglie $(x_i)_{i \in I}$ tali che $x_i \in M_i$ per ogni $i \in I$ e quasi tutti gli x_i sono zero. Se si elimina la restrizione sul numero degli elementi x_i non nulli, si ottiene il *prodotto diretto* $\prod_{i \in I} M_i$. La somma diretta e il prodotto diretto coincidono se l'insieme degli indici I è finito, ma non altrimenti, in generale.

Supponiamo che l'anello A sia un prodotto diretto $\prod_{i=1}^{n} A_i$ (Capitolo 1). Allora l'insieme di tutti gli elementi di A della forma

$$(0, \dots, 0, a_i, 0, \dots, 0)$$

con $a_i \in A_i$ è un ideale $\mathfrak{a}_i$ di A (esso *non* è un subanello di A — tranne in casi banali — poiché non contiene l'unità di A). L'anello A, considerato come A-modulo, è la somma diretta degli ideali $\mathfrak{a}_1, \dots, \mathfrak{a}_n$. Viceversa, data una decomposizione di moduli

$$A = \mathfrak{a}_1 \oplus \qquad \oplus \mathfrak{a}_n$$

di A come somma diretta di ideali, si ha

$$A \cong \prod_{i=1}^{n} (A/\mathfrak{b}_i)$$

dove $\mathfrak{b}_i = \bigoplus_{j \neq i} \mathfrak{a}_j$. Ogni ideale $\mathfrak{a}_i$ è un anello (isomorfo ad $A/\mathfrak{b}_i$). L'elemento unità e_i di $\mathfrak{a}_i$ è un idempotente in A, e $\mathfrak{a}_i = (e_i)$.

Moduli finitamente generati

Un A-modulo *libero* è un A-modulo isomorfo ad uno della forma $\bigoplus_{i \in I} M_i$, dove ciascun $M_i \cong A$ (come A-modulo). Si usa talvolta la notazione $A^{(I)}$. Un A-modulo libero finitamente generato è pertanto isomorfo ad $A \oplus \ldots \oplus A$ (n addendi), che si denota con A^n. (Per convenzione, A^0 è il modulo nullo, denotato con 0.)

Proposizione 2.3. *M è un A-modulo finitamente generato $\Leftrightarrow$ M è isomorfo ad un quoziente di A^n per qualche intero $n > 0$.*

Dimostrazione. $\Rightarrow$: Siano $x_1, \ldots, x_n$ un sistema di generatori di M. Definiamo $\phi\colon A^n \to M$ ponendo $\phi(a_1, \ldots, a_n) = a_1x_1 + \quad + a_nx_n$. Allora ϕ è un omomorfismo di A-moduli *sopra* M, e pertanto $M \cong A^n/\operatorname{Ker}(\phi)$.

$\Leftarrow$: Si ha un omomorfismo di A-moduli ϕ di A^n su M. Se $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (l'elemento 1 essendo all'i-esimo posto), allora gli e_i $(1 \leqslant i \leqslant n)$ generano A^n, quindi gli elementi $\phi(e_i)$ generano M. ■

Proposizione 2.4. *Sia M un A-modulo finitamente generato, sia $\mathfrak{a}$ un ideale di A, e sia ϕ un endomorfismo di A-moduli di M tale che $\phi(M) \subseteq \mathfrak{a}M$. Allora ϕ soddisfa ad un'equazione della forma*

$$\phi^n + a_1\phi^{n-1} + \qquad + a_n = 0$$

dove gli a_i sono elementi di $\mathfrak{a}$.

Dimostrazione. Siano $x_1, \ldots, x_n$ un sistema di generatori di M. Allora ogni $\phi(x_i) \in \mathfrak{a}M$, sicché si ha, diciamo, $\phi(x_i) = \sum_{j=1}^{n} a_{ij}x_j$ $(1 \leqslant i \leqslant n;\ a_{ij} \in \mathfrak{a})$, ossia:

$$\sum_{j=1}^{n} (\delta_{ij}\phi - a_{ij})x_j = 0$$

dove δ_{ij} è il delta di Kronecker. Moltiplicando a sinistra per l'aggiunta della matrice $(\delta_{ij}\phi - a_{ij})$ si ha che det $(\delta_{ij}\phi - a_{ij})$ annulla ciascun x_i, dunque è l'endomorfismo nullo di M. Sviluppando il determinante, si ottiene un'equazione della forma richiesta. ■

Corollario 2.5. *Sia M un A-modulo finitamente generato e sia $\mathfrak{a}$ un ideale di A tale che $\mathfrak{a}M = M$. Allora esiste un elemento $x \equiv 1 \pmod{\mathfrak{a}}$ tale che $xM = 0$.*

Dimostrazione. Basta prendere $\phi =$ identità e $x = 1 + a_1 + \cdots + a_n$ nella (2.4). ∎

Proposizione 2.6. (lemma di Nakayama). *Sia M un A-modulo finitamente generato e $\mathfrak{a}$ un ideale di A contenuto nel radicale di Jacobson $\mathfrak{R}$ di A. Allora $\mathfrak{a}M = M$ implica $M = 0$.*

Prima dimostrazione. Da (2.5) si ha $xM = 0$ per qualche $x \equiv 1 \pmod{\mathfrak{R}}$. In virtú di (1.9) x è invertibile in A, dunque $M = x^{-1}xM = 0$. ∎

Seconda dimostrazione. Supponiamo $M \neq 0$, e siano $u_1, \ldots, u_n$ un sistema minimale di generatori di M. Allora $u_n \in \mathfrak{a}M$, sicché si ha un'equazione della forma $u_n = a_1u_1 + \cdots + a_nu_n$, con $a_i \in \mathfrak{a}$. Dunque

$$(1 - a_n)u_n = a_1u_1 + \cdots + a_{n-1}u_{n-1};$$

poiché $a_n \in \mathfrak{R}$, in virtú di (1.9) $1 - a_n$ è invertibile in A. Ne segue che u_n appartiene al sottomodulo di M generato da $u_1, \ldots, u_{n-1}$: ciò è una contraddizione. ∎

Corollario 2.7. *Sia M un A-modulo finitamente generato, N un sottomodulo di M, $\mathfrak{a} \subseteq \mathfrak{R}$ un ideale. Allora $M = \mathfrak{a}M + N \Rightarrow M = N$.*

Dimostrazione. Basta applicare (2.6) a M/N, osservando che $\mathfrak{a}(M/N) = (\mathfrak{a}M + N)/N$. ∎

Sia A un anello locale, $\mathfrak{m}$ il suo ideale massimale, $k = A/\mathfrak{m}$ il suo campo residuo. Sia M un A-modulo finitamente generato. $M/\mathfrak{m}M$ è annullato da $\mathfrak{m}$, dunque è in modo naturale un $A/\mathfrak{m}$-modulo, ossia, un k-spazio vettoriale, e come tale ha dimensione finita.

Proposizione 2.8. *Siano x_i $(1 \leqslant i \leqslant n)$ elementi di M le cui immagini in $M/\mathfrak{m}M$ formano una base di tale spazio vettoriale. Allora gli x_i generano M.*

Dimostrazione. Sia N il sottomodulo di M generato dagli elementi x_i. Allora l'applicazione composta $N \to M \to M/\mathfrak{m}M$ manda N su $M/\mathfrak{m}M$, dunque $N + \mathfrak{m}M = M$, da cui $N = M$ in virtú di (2.7). ∎

Successioni esatte

Una successione di A-moduli e di A-omomorfismi

(0) $$\to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to$$

si dice *esatta in* M_i se $\mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$. La successione è *esatta* se è esatta in ciascun M_i. In particolare:

(1) $$0 \to M' \xrightarrow{f} M \text{ è esatta} \Leftrightarrow f \text{ è iniettivo;}$$

(2) $$M \xrightarrow{g} M'' \to 0 \text{ è esatta} \Leftrightarrow g \text{ è suriettivo;}$$

(3) $$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \text{ è esatta} \Leftrightarrow f \text{ è iniettivo,}$$

g è suriettivo e g induce un isomorfismo di $\mathrm{Coker}(f) = M/f(M')$ su M''.

Una successione del tipo (3) prende il nome di *successione esatta corta*. Una qualsiasi successione esatta lunga (0) può essere spezzata in successioni esatte corte: se $N_i = \mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$, si ottengono successioni esatte corte $0 \to N_i \to M_i \to N_{i+1} \to 0$ per ogni i.

Proposizione 2.9. i) *Sia*

(4) $$M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$$

una successione di A-moduli ed omomorfismi. Allora la successione (4) *è esatta* $\Leftrightarrow$ *per ogni A-modulo N, la successione*

(4') $$0 \to \mathrm{Hom}(M'', N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}(M', N)$$

è esatta.

ii) *Sia*

(5) $$0 \to N' \xrightarrow{u} N \xrightarrow{v} N''$$

una successione di A-moduli ed omomorfismi. Allora la successione (5) *è esatta* $\Leftrightarrow$ *per ogni A-modulo M, la successione*

(5') $$0 \to \mathrm{Hom}(M, N') \xrightarrow{\bar{u}} \mathrm{Hom}(M, N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N'')$$

è esatta.

Tutte le parti di questa proposizione sono facili esercizi. Per esempio, supponiamo che la (4') sia esatta per ogni N. Innanzitutto, poiché $\bar{v}$ è iniettivo per ogni N, v risulta suriettivo. Inoltre, si ha $\bar{u} \circ \bar{v} = 0$, ossia, $f \circ v \circ u = 0$ per ogni $f: M'' \to N$. Prendendo $N = M''$ ed f uguale all'applicazione identica, si ha che $v \circ u = 0$, da cui $\mathrm{Im}(u) \subseteq \mathrm{Ker}(v)$. Prendiamo poi $N = M/\mathrm{Im}(u)$ e sia $\phi: M \to N$ la proiezione. Allora $\phi \in \mathrm{Ker}(\bar{u})$, sicché esiste un omomorfismo $\psi: M'' \to N$ tale che $\phi = \psi \circ v$. Di conseguenza, $\mathrm{Im}(u) = \mathrm{Ker}(\phi) \supseteq \mathrm{Ker}(v)$. ■

Proposizione 2.10. *Sia*

$$\begin{array}{ccccccccc} 0 & \to & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \to & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \to & N' & \xrightarrow[u']{} & N & \xrightarrow[v']{} & N'' & \to & 0 \end{array}$$

un diagramma commutativo di A-moduli ed omomorfismi, con le righe esatte. Allora esiste una successione esatta

$$\begin{gathered} 0 \to \mathrm{Ker}(f') \xrightarrow{\bar{u}} \mathrm{Ker}(f) \xrightarrow{\bar{v}} \mathrm{Ker}(f'') \xrightarrow{d} \\ \mathrm{Coker}(f') \xrightarrow{\bar{u}'} \mathrm{Coker}(f) \xrightarrow{\bar{v}'} \mathrm{Coker}(f'') \to 0 \end{gathered} \tag{6}$$

in cui $\bar{u}$, $\bar{v}$ sono restrizioni di u, v e $\bar{u}'$, $\bar{v}'$ sono indotti da u', v'.

L'*omomorfismo bordo* d è definito nel modo seguente: se $x'' \in \mathrm{Ker}(f'')$, si ha $x'' = v(x)$ per qualche $x \in M$, e $v'(f(x)) = f''(v(x)) = 0$, da cui $f(x) \in \mathrm{Ker}(v') = \mathrm{Im}(u')$, sicché $f(x) = u'(y')$ per qualche $y' \in N'$. Allora $d(x'')$ è definito come l'immagine di y' in $\mathrm{Coker}(f')$. La verifica che d è ben definito, e che la successione (6) è esatta, è un semplice esercizio di "caccia al diagramma" che lasciamo al lettore. ■

Osservazione. La (2.10) è un caso speciale della successione esatta di omologia dell'algebra omologica.

Sia C una classe di A-moduli e sia λ una funzione su C a valori in $\mathbf{Z}$ (o, più in generale, a valori in un gruppo abeliano G). La funzione λ è *additiva* se, per ogni successione esatta corta (3) in cui tutti i termini appartengono a C, si ha $\lambda(M') - \lambda(M) + \lambda(M'') = 0$.

Esempio. Sia A un campo k, e sia C la classe di tutti i k-spazi vettoriali V di dimensione finita. Allora $V \mapsto \dim V$ è una funzione additiva su C.

Proposizione 2.11. *Sia* $0 \to M_0 \to M_1 \to \ldots \to M_n \to 0$ *una successione esatta di* A*-moduli in cui tutti i moduli* M_i *e i nuclei di tutti gli omomorfismi appartengono a* C. *Allora per una qualsiasi funzione additiva su* C *si ha:*

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0.$$

Dimostrazione. Spezziamo la successione data in successioni esatte corte

$$0 \to N_i \to M_i \to N_{i+1} \to 0$$

($N_0 = N_{n+1} = 0$). Allora si ha $\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1})$. Ora prendiamo la somma alternata dei $\lambda(M_i)$, e tutto si cancella. ■

Prodotto tensoriale di moduli

Siano M, N, P tre A-moduli. Un'applicazione $f\colon M \times N \to P$ si dice A*-bilineare* se per ogni $x \in M$ l'applicazione $y \mapsto f(x, y)$ di N in P è A-lineare, e per ogni $y \in N$ l'applicazione $x \mapsto f(x, y)$ di M in P è A-lineare.

Costruiremo un A-modulo T, chiamato il *prodotto tensoriale* di M e N, con la proprietà che le applicazioni A-bilineari $M \times N \to P$ sono in corrispondenza biunivoca naturale con le applicazioni A-lineari $T \to P$, per ogni A-modulo P. Piú precisamente:

Proposizione 2.12. *Siano* M, N A*-moduli. Allora esiste una coppia* (T, g) *costituita da un* A*-modulo* T *e da un'applicazione* A*-bilineare* $g\colon M \times N \to T$, *con la seguente proprietà:*

Dati un qualsiasi A*-modulo* P *e un'arbitraria applicazione* A*-bilineare* $f\colon M \times N \to P$, *esiste un'unica applicazione* A*-lineare* $f'\colon T \to P$ *tale che* $f = f' \circ g$ *(in altre parole, ogni funzione bilineare su* $M \times N$ *si fattorizza tramite* T*).*

Inoltre, se (T, g) *e* (T', g') *sono due coppie con tale proprietà, allora esiste un unico isomorfismo* $j\colon T \to T'$ *tale che* $j \circ g = g'$.

Dimostrazione. i) *Unicità.* Sostituendo (P, f) con (T', g') si ottiene un'unica applicazione A-lineare $j\colon T \to T'$ tale che $g' = j \circ g$. Scambiando i ruoli di T e T', si ottiene un'applicazione A-lineare $j'\colon T' \to T$ tale che $g = j' \circ g'$. Ciascuna delle composizioni $j \circ j', j' \circ j$ deve essere l'identità, e pertanto j è un isomorfismo.

ii) *Esistenza*. Denotiamo con C l'A-modulo libero $A^{(M \times N)}$. Gli elementi di C sono combinazioni lineari formali di elementi di $M \times N$ a coefficienti in A, ossia, sono espressioni della forma $\sum_{i=1}^{n} a_i \cdot (x_i, y_i)$ $(a_i \in A, x_i \in M, y_i \in N)$.

Sia D il sottomodulo di C generato da tutti gli elementi di C dei seguenti tipi:

$$\begin{gathered}(x + x', y) - (x, y) - (x', y) \\ (x, y + y') - (x, y) - (x, y') \\ (ax, y) - a \quad (x, y) \\ (x, ay) - a \cdot (x, y).\end{gathered}$$

Poniamo $T = C/D$. Per ogni elemento (x, y) della base di C, denotiamo con $x \otimes y$ la sua immagine in T. Allora T è generato dagli elementi della forma $x \otimes y$, e in virtú delle nostre definizioni si ha:

$$\begin{gathered}(x + x') \otimes y = x \otimes y + x' \otimes y, \quad x \otimes (y + y') = x \otimes y + x \otimes y', \\ (ax) \otimes y = x \otimes (ay) = a(x \otimes y).\end{gathered}$$

In modo equivalente, l'applicazione $g: M \times N \to T$ definita da $g(x, y) = x \otimes y$ è A-bilineare.

Una qualsiasi applicazione f di $M \times N$ in un A-modulo P si estende per linearità ad un omomorfismo di A-moduli $\bar{f}: C \to P$. Supponiamo in particolare che f sia A-bilineare. Allora, in virtú delle definizioni sopra date, $\bar{f}$ si annulla su tutti i generatori di D, dunque su tutto D, e pertanto induce un ben definito A-omomorfismo f' di $T = C/D$ in P tale che $f'(x \otimes y) = f(x, y)$. L'applicazione f' è definita univocamente da tale condizione, e pertanto la coppia (T, g) soddisfa alle condizioni della proposizione. ■

Osservazioni. i) Il modulo T sopra costruito è chiamato il ***prodotto tensoriale*** di M e N, e si denota con $M \otimes_A N$, o soltanto con $M \otimes N$ se non vi è ambiguità sull'anello A. Esso è generato come A-modulo dai "prodotti" $x \otimes y$. Se $(x_i)_{i \in I}, (y_j)_{j \in J}$ sono famiglie di generatori di M, N rispettivamente, allora gli elementi $x_i \otimes y_j$ generano $M \otimes N$. In particolare, se M e N sono finitamente generati, tale è $M \otimes N$.

ii) La notazione $x \otimes y$ è chiaramente ambigua a meno che non si specifichi il prodotto tensoriale al quale si riferisce. Siano M', N' sottomoduli di M, N rispettivamente, e sia $x \in M'$ e $y \in N'$. Allora può accadere che $x \otimes y$ come elemento di $M \otimes N$ sia zero, mentre $x \otimes y$ *come elemento di* $M' \otimes N'$ sia diverso da zero. Per esempio, prendiamo $A = \mathbf{Z}$, $M = \mathbf{Z}$, $N = \mathbf{Z}/2\mathbf{Z}$, e sia M' il sottomodulo $2\mathbf{Z}$ di $\mathbf{Z}$, mentre $N' = N$. Sia x l'elemento non nullo di N e consideriamo $2 \otimes x$. Come elemento di $M \otimes N$, esso è zero poiché $2 \otimes x = 1 \otimes \otimes 2x = 1 \otimes 0 = 0$. Ma come elemento di $M' \otimes N'$ è diverso da zero. (Cfr. l'esempio discusso dopo (2.18).)

Tuttavia, vale il seguente risultato:

Corollario 2.13. *Siano $x_i \in M, y_i \in N$ tali che $\sum x_i \otimes y_i = 0$ in $M \otimes N$. Allora esistono sottomoduli finitamente generati M_0 di M e N_0 di N tali che $\sum x_i \otimes y_i = 0$ in $M_0 \otimes N_0$.*

Dimostrazione. Se $\sum x_i \otimes y_i = 0$ in $M \otimes N$, allora con le notazioni usate nella dimostrazione di (2.12) si ha $\sum (x_i, y_i) \in D$, e pertanto l'elemento $\sum (x_i, y_i)$ è una somma finita di generatori di D. Sia M_0 il sottomodulo di M generato dagli x_i e da tutti gli elementi di M che compaiono come prime coordinate in tali generatori di D, e definiamo N_0 in modo simile. Allora $\sum x_i \otimes y_i = 0$ come elemento di $M_0 \otimes N_0$. ■

iii) Non avremo più bisogno di usare la costruzione del prodotto tensoriale data in (2.12), e il lettore può anche dimenticarla, se preferisce. Ciò che è essenziale ricordare è la proprietà che definisce il prodotto tensoriale.

iv) Invece di partire dalle applicazioni bilineari, saremmo potuti partire dalle applicazioni multilineari $f: M_1 \times \ldots \times M_r \to P$ definite allo stesso modo (ossia, lineari in ciascuna variabile). Seguendo la dimostrazione di (2.12) otterremmo alla fine un "prodotto multitensoriale" $T = M_1 \otimes \ldots \otimes M_r$, generato da tutti i prodotti $x_1 \otimes \ldots \otimes \otimes x_r$ $(x_i \in M_i, 1 \leqslant i \leqslant r)$. I dettagli possono essere lasciati al lettore; il risultato corrispondente a (2.12) è il seguente:

Proposizione 2.12*. *Siano $M_1, \ldots, M_r$ A-moduli. Allora esiste una coppia (T, g) costituita da un A-modulo T ed un'applicazione A-multilineare $g: M_1 \times \quad \times M_r \to T$ con la seguente proprietà:*

Dati un qualsiasi A-modulo P ed un'arbitraria applicazione A-multilineare $f: M_1 \times \ldots \times M_r \to P$, esiste un unico A-omomorfismo $f': T \to P$ tale che $f' \circ g = f$.

Inoltre, se (T, g) e (T', g') sono due coppie con tale proprietà, allora esiste un unico isomorfismo $j: T \to T'$ tale che $j \circ g = g'$. ■

Sussistono vari cosiddetti "isomorfismi canonici", alcuni dei quali vengono qui stabiliti:

Proposizione 2.14. *Siano M, N, P A-moduli. Allora esistono isomorfismi univocamente determinati:*

i) $M \otimes N \to N \otimes M$
ii) $(M \otimes N) \otimes P \to M \otimes (N \otimes P) \to M \otimes N \otimes P$
iii) $(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$
iv) $A \otimes M \to M$

tali che, rispettivamente,

a) $x \otimes y \mapsto y \otimes x$
b) $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z) \mapsto x \otimes y \otimes z$
c) $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$
d) $a \otimes x \mapsto ax$.

Dimostrazione. In ciascuno dei casi in questione si tratta di provare che le applicazioni sopra descritte sono ben definite. La tecnica consiste nel costruire opportune applicazioni bilineari o multilineari, e usare la proprietà di definizione (2.12) o (2.12*) per dedurre l'esistenza di omomorfismi di prodotti tensoriali. Dimostreremo una parte di ii) come esempio del metodo da seguire, e lasceremo il resto della dimostrazione al lettore.

Costruiremo degli omomorfismi

$$(M \otimes N) \otimes P \xrightarrow{f} M \otimes N \otimes P \xrightarrow{g} (M \otimes N) \otimes P$$

tali che $f((x \otimes y) \otimes z) = x \otimes y \otimes z$ e $g(x \otimes y \otimes z) = (x \otimes y) \otimes z$, per ogni $x \in M, y \in N, z \in P$.

Per costruire f, fissiamo un elemento $z \in P$. L'applicazione $(x, y) \mapsto x \otimes y \otimes z$ $(x \in M, y \in N)$ è bilineare in x e y e pertanto induce un omomorfismo $f_z: M \otimes N \to M \otimes N \otimes P$ tale che $f_z(x \otimes y) = x \otimes y \otimes z$. Successivamente, consideriamo l'applicazione $(t, z) \mapsto f_z(t)$ di $(M \otimes N) \times P$ in $M \otimes N \otimes P$. Essa è bilineare in t e z e pertanto induce un omomorfismo

$$f: (M \otimes N) \otimes P \to M \otimes N \otimes P$$

tale che $f((x \otimes y) \otimes z) = x \otimes y \otimes z$.

Per costruire g, consideriamo l'applicazione $(x, y, z) \mapsto (x \otimes y) \otimes z$ di $M \times N \times P$ in $(M \otimes N) \otimes P$. Essa è lineare in ciascuna variabile e pertanto induce un omomorfismo

$$g: M \otimes N \otimes P \to (M \otimes N) \otimes P$$

tale che $g(x \otimes y \otimes z) = (x \otimes y) \otimes z$.

Chiaramente $f \circ g$ e $g \circ f$ sono applicazioni identiche, sicché f e g sono isomorfismi. ■

Esercizio 2.15. *Siano A, B anelli, M un A-modulo, P un B-modulo e N un (A, B)-bimodulo (ossia, N è simultaneamente un A-modulo e un B-modulo e le due strutture sono compatibili nel senso che $a(xb) = (ax)b$ per ogni $a \in A$, $b \in B$, $x \in N$). Allora $M \otimes_A N$ è in modo naturale un B-modulo, $N \otimes_B P$ è un A-modulo, e si ha*

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P).$$

Siano $f: M \to M'$, $g: N \to N'$ omomorfismi di A-moduli. Definiamo $h: M \times N \to M' \otimes N'$ ponendo $h(x, y) = f(x) \otimes g(y)$. Si verifica facilmente che h è A-bilineare e pertanto induce un omomorfismo di A-moduli

$$f \otimes g: M \otimes N \to M' \otimes N'$$

tale che

$$(f \otimes g)(x \otimes y) = f(x) \otimes g(y) \qquad (x \in M, y \in N).$$

Siano $f': M' \to M''$ e $g': N' \to N''$ omomorfismi di A-moduli. Allora chiaramente gli omomorfismi $(f' \circ f) \otimes (g' \circ g)$ e $(f' \otimes g') \circ (f \otimes g)$ coincidono su tutti gli elementi della forma $x \otimes y$ in $M \otimes N$. Poiché tali elementi generano $M \otimes N$, ne segue che

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g).$$

Restrizione ed estensione degli scalari

Sia $f: A \to B$ un omomorfismo di anelli e sia N un B-modulo. Allora N possiede una struttura di A-modulo definita nel modo seguente: se $a \in A$ e $x \in N$, allora ax viene definito come $f(a)x$. Tale A-modulo si dice ottenuto da N per *restrizione degli scalari*. In particolare, f definisce in tal modo una struttura di A-modulo su B.

Proposizione 2.16. *Supponiamo che N sia finitamente generato come B-modulo e che B sia finitamente generato come A-modulo. Allora N è finitamente generato come A-modulo.*

Dimostrazione. Siano $y_1, \ldots, y_n$ un sistema di generatori di N sopra B e $x_1, \ldots, x_m$ un sistema di generatori di B come A-modulo. Allora gli mn prodotti $x_i y_j$ generano N sopra A. ■

Sia ora M un A-modulo. Poiché, come abbiamo appena visto, B può essere considerato come un A-modulo, si può formare l'A-modulo $M_B = B \otimes_A M$. Infatti M_B possiede una struttura di B-modulo tale che $b(b' \otimes x) = bb' \otimes x$ per ogni $b, b' \in B$ e per ogni $x \in M$. Il B-modulo M_B si dice ottenuto da M per *estensione degli scalari*.

Proposizione 2.17. *Se M è un A-modulo finitamente generato, allora M_B è un B-modulo finitamente generato.*

Dimostrazione. Se $x_1, \ldots, x_m$ generano M sopra A, allora gli elementi $1 \otimes x_i$ generano M_B su B. ∎

Proprietà di esattezza del prodotto tensoriale

Sia $f\colon M \times N \to P$ un'applicazione A-bilineare. Per ogni $x \in M$ l'applicazione $y \mapsto f(x, y)$ di N in P è A-lineare, sicché f dà origine ad un'applicazione $M \to \operatorname{Hom}(N, P)$ che è A-lineare poiché f è lineare nella variabile x. Viceversa, un qualsiasi A-omomorfismo $\phi\colon M \to \operatorname{Hom}_A(N, P)$ definisce un'applicazione bilineare, precisamente $(x, y) \mapsto \phi(x)(y)$. Dunque l'insieme S delle applicazioni A-bilineari $M \times N \to P$ è in corrispondenza biunivoca naturale con $\operatorname{Hom}(M, \operatorname{Hom}(N, P))$. D'altra parte S è in corrispondenza biunivoca con $\operatorname{Hom}(M \otimes N, P)$, in virtú della proprietà che definisce il prodotto tensoriale. Si ha dunque un isomorfismo canonico:

$$\operatorname{Hom}(M \otimes N, P) \cong \operatorname{Hom}(M, \operatorname{Hom}(N, P)). \tag{1}$$

Proposizione 2.18. *Sia*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{2}$$

una successione esatta di A-moduli ed omomorfismi, e sia N un A-modulo arbitrario. Allora la successione

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \to 0 \tag{3}$$

(dove 1 *denota l'applicazione identica su N) è esatta.*

Dimostrazione. Denotiamo con E la successione (2) e con $E \otimes N$ la successione (3). Sia P un A-modulo arbitrario. Poiché (2) è esatta, la successione $\operatorname{Hom}(E, \operatorname{Hom}(N, P))$ è esatta in virtú di (2.9); dunque, stante la (1), la successione $\operatorname{Hom}(E \otimes N, P)$ è esatta. Ancora da (2.9), segue che $E \otimes N$ è esatta. ∎

Osservazioni. i) Poniamo $T(M) = M \otimes N$ e $U(P) = \mathrm{Hom}(N,P)$. Allora (1) prende la forma $\mathrm{Hom}(T(M), P) = \mathrm{Hom}(M, U(P))$ per tutti gli A-moduli M e P. Nel linguaggio della teoria delle categorie (*abstract nonsense*), il funtore T è l'aggiunto a sinistra di U, e U è l'aggiunto a destra di T. La dimostrazione di (2.18) fa vedere che un qualsiasi funtore che è un aggiunto a sinistra risulta esatto a destra. Similmente, un qualsiasi funtore che è un aggiunto a destra risulta esatto a sinistra.

ii) In generale, *non* è vero che, se $M' \to M \to M''$ è una successione esatta di A-moduli e di omomorfismi, la successione $M' \otimes N \to M \otimes N \to M'' \otimes N$ ottenuta tensorizzando con un A-modulo arbitrario N è esatta.

Esempio. Prendiamo $A = \mathbf{Z}$ e consideriamo la successione esatta $0 \to \mathbf{Z} \xrightarrow{f} \mathbf{Z}$, dove $f(x) = 2x$ per ogni $x \in \mathbf{Z}$. Se tensorizziamo con $N = \mathbf{Z}/2\mathbf{Z}$, la successione $0 \to \mathbf{Z} \otimes N \xrightarrow{f \otimes 1} \mathbf{Z} \otimes N$ *non* è esatta, poiché per ogni $x \otimes y \in \mathbf{Z} \otimes N$ si ha

$$(f \otimes 1)(x \otimes y) = 2x \otimes y = x \otimes 2y = x \otimes 0 = 0,$$

sicché $f \otimes 1$ è l'applicazione nulla, mentre $\mathbf{Z} \otimes N \neq 0$.

Il funtore $T_N \colon M \mapsto M \otimes_A N$ sulla categoria degli A-moduli ed omomorfismi (di A-moduli) non è quindi esatto in generale. Se T_N è esatto, ossia, se la tensorizzazione con N trasforma tutte le successioni esatte in successioni esatte, allora si dice che N è un A-modulo *piatto*.

Proposizione 2.19. *Le seguenti proprietà sono equivalenti, per un A-modulo N:*

i) *N è piatto.*

ii) *Se $0 \to M' \to M \to M'' \to 0$ è una qualsiasi successione esatta di A-moduli, la successione tensorizzata $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ è esatta.*

iii) *Se $f \colon M' \to M$ è iniettivo, allora $f \otimes 1 \colon M' \otimes N \to M \otimes N$ è iniettivo.*

iv) *Se $f \colon M' \to M$ è iniettivo e M, M' sono finitamente generati, allora $f \otimes 1 \colon M' \otimes N \to M \otimes N$ è iniettivo.*

Dimostrazione. i) $\Leftrightarrow$ ii) spezzando una successione esatta lunga in successioni esatte corte.

ii) $\Leftrightarrow$ iii) in virtú di (2.18).

iii) $\Rightarrow$ iv) è banale.

iv) $\Rightarrow$ iii). Sia $f: M' \to M$ un omomorfismo iniettivo e sia $u = \sum x'_i \otimes y_i \in \operatorname{Ker}(f \otimes 1)$, sicché $\sum f(x'_i) \otimes y_i = 0$ in $M \otimes N$. Sia M'_0 il sottomodulo di M' generato dagli elementi x'_i e denotiamo con u_0 la somma $\sum x'_i \otimes y_i$ come elemento di $M'_0 \otimes N$. Stante (2.14), esiste un sottomodulo finitamente generato M_0 di M contenente $f(M'_0)$ e tale che $\sum f(x'_i) \otimes y_i = 0$ come elemento di $M_0 \otimes N$. Se $f_0: M'_0 \to M_0$ è la restrizione di f, ciò significa che $(f_0 \otimes 1)(u_0) = 0$. Poiché M_0 e M'_0 sono finitamente generati, $f_0 \otimes 1$ è iniettivo e pertanto $u_0 = 0$, da cui $u = 0$. ■

Esercizio 2.20. *Se $f: A \to B$ è un omomorfismo di anelli e M è un A-modulo piatto, allora $M_B = B \otimes_A M$ è un B-modulo piatto.* (Usare gli isomorfismi canonici (2.14), (2.15).)

Algebre

Sia $f: A \to B$ un omomorfismo di anelli. Se $a \in A$ e $b \in B$, definiamo un prodotto

$$ab = f(a)b.$$

Con questa definizione di moltiplicazione scalare l'anello B diventa un A-modulo (è un esempio particolare di restrizione di scalari). Allora B possiede una struttura di A-modulo e una struttura di anello, e queste due strutture sono compatibili in un senso che il lettore sarà in grado di formulare da solo. L'anello B, dotato di tale struttura di A-modulo, prende il nome di *A-algebra*. Dunque una A-algebra è, per definizione, un anello B insieme con un omomorfismo di anelli $f: A \to B$.

Osservazioni. i) In particolare, se A è un campo K (e $B \neq 0$) allora f è iniettivo, in virtú di (1.2), e pertanto K può venire identificato in modo canonico con la sua immagine in B. Dunque una K-algebra (essendo K un campo) è in realtà un anello che contiene K come un subanello.

ii) Sia A un anello arbitrario. Poiché A possiede un elemento unità, esiste un unico omomorfismo dell'anello degli interi $\mathbf{Z}$ in A, precisamente $n \mapsto n \quad 1$. Dunque ogni anello è automaticamente una $\mathbf{Z}$-algebra.

Siano $f: A \to B$, $g: A \to C$ due omomorfismi di anelli. Un *omomorfismo di A-algebre $h: B \to C$* è un omomorfismo di anelli che è anche un omomorfismo di A-moduli. Il lettore dovrebbe verificare che h è un omomorfismo di A-algebre se, e soltanto se, $h \circ f = g$.

Un omomorfismo di anelli $f: A \to B$ è *finito*, e B è una A-algebra *finita*, se B è un A-modulo finitamente generato. L'omomorfismo f è *di tipo finito*, e B è una *A-algebra finitamente generata*, se esiste un insieme finito di elementi $x_1, \dots, x_n$ in B tali che ogni elemento di B può essere espresso come un polinomio in $x_1, \dots, x_n$ a coefficienti in $f(A)$; oppure, in modo equivalente, se esiste un omomorfismo di A-algebre da un anello di polinomi $A[t_1, \dots, t_n]$ *sopra* B.*

Un anello A si dice *finitamente generato* se è una Z-algebra finitamente generata. Ciò significa che esiste un insieme finito di elementi $x_1, \dots, x_n$ in A tali che ogni elemento di A può essere espresso come un polinomio negli x_i a coefficienti interi.

Prodotto tensoriale di algebre

Siano B, C due A-algebre, $f: A \to B$, $g: A \to C$ gli omomorfismi corrispondenti. Poiché B e C sono A-moduli, possiamo formare il loro prodotto tensoriale $D = B \otimes_A C$, il quale è un A-modulo. Definiremo ora una moltiplicazione su D.

Consideriamo l'applicazione $B \times C \times B \times C \to D$ definita da

$$(b, c, b', c') \mapsto bb' \otimes cc'.$$

Essa è A-lineare in ciascun fattore e pertanto, in virtú di (2.12*), induce un omomorfismo di A-moduli

$$B \otimes C \otimes B \otimes C \to D,$$

e quindi, stante (2.14), un omomorfismo di A-moduli

$$D \otimes D \to D$$

il quale a sua volta corrisponde, in virtú di (2.12), ad un'applicazione A-bilineare

$$\mu: D \times D \to D$$

tale che

$$\mu(b \otimes c, b' \otimes c') = bb' \otimes cc'.$$

* Inoltre un omomorfismo di anelli $f: A \to B$ è *piatto*, e B è una A-algebra *piatta*, se B è un A-modulo piatto.

Naturalmente, avremmo potuto scrivere direttamente tale formula, ma senza una argomentazione quale quella sopra sviluppata, non ci sarebbe stata alcuna garanzia che μ era ben definita.

Abbiamo definito dunque una moltiplicazione sul prodotto tensoriale $D = B \otimes_A C$: per elementi della forma $b \otimes c$ essa è data da

$$(b \otimes c)(b' \otimes c') = bb' \otimes cc',$$

e in generale da

$$\left(\sum_i (b_i \otimes c_i)\right)\left(\sum_j (b'_j \otimes c'_j)\right) = \sum_{i,j} (b_i b'_j \otimes c_i c'_j).$$

Il lettore dovrebbe verificare che, con tale moltiplicazione, D risulta un anello commutativo, con elemento unità $1 \otimes 1$. Inoltre, D è una A-algebra: l'applicazione $a \mapsto f(a) \otimes 1 = 1 \otimes g(a)$ è un omomorfismo di anelli $A \to D$. Infatti si ha un diagramma commutativo di omomorfismi di anelli

$$\begin{tikzcd} & B \arrow[dr, "u"] & \\ A \arrow[ur, "f"] \arrow[dr, "g"'] & & D \\ & C \arrow[ur, "v"'] & \end{tikzcd}$$

in cui u, v sono definiti rispettivamente da: $u(b) = b \otimes 1$, $v(c) = 1 \otimes c$.

Esercizi

1. Provare che $(\mathbf{Z}/m\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/n\mathbf{Z}) = 0$ se m, n sono coprimi.
2. Sia A un anello, $\mathfrak{a}$ un ideale, M un A-modulo. Dimostrare che $(A/\mathfrak{a}) \otimes_A M$ è isomorfo a $M/\mathfrak{a}M$.
[Tensorizzare la successione esatta $0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$ con M.]
3. Siano A un anello locale, M e N A-moduli finitamente generati. Provare che se $M \otimes N = 0$, allora $M = 0$ oppure $N = 0$.
[Sia $\mathfrak{m}$ l'ideale massimale, $k = A/\mathfrak{m}$ il campo residuo. Poniamo $M_k = k \otimes_A M \cong M/\mathfrak{m}M$ (cfr. Esercizio 2). In virtù del lemma di Nakayama, $M_k = 0 \Rightarrow M = 0$. Ma $M \otimes_A N = 0 \Rightarrow (M \otimes_A N)_k =$

$= 0 \Rightarrow M_k \otimes_k N_k = 0 \Rightarrow M_k = 0$ oppure $N_k = 0$, poiché M_k, N_k sono spazi vettoriali sopra un campo.]

4. Sia $(M_i)_{i \in I}$ una qualsiasi famiglia di A-moduli, e sia M la loro somma diretta. Dimostrare che M è piatto $\Leftrightarrow$ ogni M_i è piatto.

5. Sia $A[x]$ l'anello dei polinomi in una indeterminata sopra un anello A. Provare che $A[x]$ è una A-algebra piatta. [Usare l'Esercizio 4.]

6. Per un A-modulo qualsiasi, denotiamo con $M[x]$ l'insieme di tutti i polinomi in x a coefficienti in M, ossia, espressioni della forma
$$m_0 + m_1 x + \quad + m_r x^r \qquad (m_i \in M).$$
Definendo il prodotto di un elemento di $A[x]$ per un elemento di $M[x]$ in modo ovvio, verificare che $M[x]$ è un $A[x]$-modulo.
Provare che $M[x] \cong A[x] \otimes_A M$.

7. Sia $\mathfrak{p}$ un ideale primo di A. Dimostrare che $\mathfrak{p}[x]$ è un ideale primo di $A[x]$. Se $\mathfrak{m}$ è un ideale massimale di A, $\mathfrak{m}[x]$ risulta un ideale massimale di $A[x]$?

8. i) Se M e N sono A-moduli piatti, allora tale risulta $M \otimes_A N$.
ii) Se B è una A-algebra piatta e N è un B-modulo piatto, allora N è piatto come A-modulo.

9. Sia $0 \to M' \to M \to M'' \to 0$ una successione esatta di A-moduli. Se M' e M'' sono finitamente generati, tale risulta anche M.

10. Sia A un anello, $\mathfrak{a}$ un ideale contenuto nel radicale di Jacobson di A; sia M un A-modulo e N un A-modulo finitamente generato, e sia $u: M \to N$ un omomorfismo. Se l'omomorfismo indotto $M/\mathfrak{a}M \to N/\mathfrak{a}N$ è suriettivo, allora u è suriettivo.

11. Sia A un anello $\neq 0$. Provare che $A^m \cong A^n \Rightarrow m = n$.
[Sia $\mathfrak{m}$ un ideale massimale di A e sia $\phi: A^m \to A^n$ un isomorfismo. Allora $1 \otimes \phi: (A/\mathfrak{m}) \otimes A^m \to (A/\mathfrak{m}) \otimes A^n$ è un isomorfismo tra spazi vettoriali di dimensioni m e n sopra il campo $k = A/\mathfrak{m}$. Dunque $m = n$.] (Cfr. Capitolo 3, Esercizio 15.)
Se $\phi: A^m \to A^n$ è suriettivo, allora $m \geqslant n$.
Se $\phi: A^m \to A^n$ è iniettivo, è vero che risulta sempre $m \leqslant n$?

12. Sia M un A-modulo finitamente generato e $\phi: M \to A^n$ un omomorfismo suriettivo. Dimostrare che $\operatorname{Ker}(\phi)$ è finitamente generato.
[Siano $e_1, \ldots, e_n$ gli elementi di una base di A^n e scegliamo degli elementi $u_i \in M$ tali che $\phi(u_i) = e_i (1 \leqslant i \leqslant n)$. Provare che M è

la somma diretta di $\mathrm{Ker}(\phi)$ e del sottomodulo generato da $u_1, \ldots, u_n$.]

13. Sia $f: A \to B$ un omomorfismo di anelli, e sia N un B-modulo. Considerando N come A-modulo mediante restrizione degli scalari, formare il B-modulo $N_B = B \otimes_A N$. Dimostrare che l'omomorfismo $g: N \to N_B$ che manda y in $1 \otimes y$ è iniettivo e che $g(N)$ è un addendo diretto di N_B.
[Definire $p: N_B \to N$ ponendo $p(b \otimes y) = by$, e provare che $N_B = \mathrm{Im}(g) \oplus \mathrm{Ker}(p)$.]

Limiti diretti

14. Un insieme parzialmente ordinato I si dice un insieme ***diretto*** se per ogni coppia di elementi i, j in I, esiste un elemento $k \in I$ tale che $i \leqslant k$ e $j \leqslant k$.

 Sia A un anello, e siano I un insieme diretto e $(M_i)_{i \in I}$ una famiglia di A-moduli indiciata da I. Per ogni coppia i, j in I tale che $i \leqslant j$, sia $\mu_{ij}: M_i \to M_j$ un A-omomorfismo, e supponiamo che siano soddisfatti i seguenti assiomi:

 (1) μ_{ii} è l'applicazione identica di M_i, per ogni $i \in I$;

 (2) $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$ ogni volta che $i \leqslant j \leqslant k$.

 Allora si dice che i moduli M_i e gli omomorfismi μ_{ij} formano un *sistema diretto* $\mathbf{M} = (M_i, \mu_{ij})$ sull'insieme diretto I.

 Costruiremo un A-modulo M chiamato il *limite diretto* del sistema diretto $\mathbf{M}$. Sia C la somma diretta degli M_i, e identifichiamo ciascun modulo M_i con la sua immagine canonica in C. Sia D il sottomodulo di C generato da tutti gli elementi della forma $x_i - \mu_{ij}(x_i)$ dove $i \leqslant j$ e $x_i \in M_i$. Poniamo $M = C/D$, e siano $\mu: C \to M$ la proiezione e μ_i la restrizione di μ a M_i.

 Il modulo M, o più precisamente la coppia costituita da M e dalla famiglia di omomorfismi $\mu_i: M_i \to M$, prende il nome di *limite diretto* del sistema diretto $\mathbf{M}$, e si scrive $\varinjlim M_i$. Dalla costruzione è chiaro che $\mu_i = \mu_j \circ \mu_{ij}$ ogni volta che $i \leqslant j$.

15. Nella situazione dell'Esercizio 14, provare che ogni elemento di M può essere scritto nella forma $\mu_i(x_i)$ per qualche $i \in I$ e per qualche $x_i \in M_i$.

 Provare inoltre che se $\mu_i(x_i) = 0$, allora esiste un indice $j \geqslant i$ tale che $\mu_{ij}(x_i) = 0$ in M_j.

16. Dimostrare che il limite diretto è caratterizzato (a meno di isomorfismi) dalla seguente proprietà:

    Sia N un A-modulo, e per ogni indice $i \in I$ sia $\alpha_i: M_i \to N$ un omomorfismo di A-moduli tale che $\alpha_i = \alpha_j \circ \mu_{ij}$ ogni volta che $i \leqslant j$. Allora esiste un unico omomorfismo $\alpha: M \to N$ tale che $\alpha_i = \alpha \circ \mu_i$ per ogni $i \in I$.

17. Sia $(M_i)_{i \in I}$ una famiglia di sottomoduli di un A-modulo, tale che per ogni coppia di indici i, j in I, esiste un indice $k \in I$ tale che $M_i + M_j \subseteq M_k$. Poniamo per definizione $i \leqslant j$ se e soltanto se $M_i \subseteq M_j$, e sia $\mu_{ij}: M_i \to M_j$ l'omomorfismo di inclusione di M_i in M_j. Dimostrare che

    $$\varinjlim M_i = \sum M_i = \bigcup M_i.$$

    In particolare, ogni A-modulo è il limite diretto della famiglia dei suoi sottomoduli finitamente generati.

18. Siano $\mathbf{M} = (M_i, \mu_{ij})$, $\mathbf{N} = (N_i, \nu_{ij})$ sistemi diretti di A-moduli sul medesimo insieme diretto. Siano M, N i limiti diretti e $\mu_i: M_i \to M$, $\nu_i: N_i \to N$ gli omomorfismi associati.

    Un *omomorfismo* $\boldsymbol{\phi}: \mathbf{M} \to \mathbf{N}$ è per definizione una famiglia di omomorfismi di A-moduli $\phi_i: M_i \to N_i$ tali che $\phi_j \circ \mu_{ij} = \nu_{ij} \circ \phi_i$ ogni volta che $i \leqslant j$. Dimostrare che $\boldsymbol{\phi}$ definisce un unico omomorfismo $\phi = \varinjlim \phi_i: M \to N$ tale che $\phi \circ \mu_i = \nu_i \circ \phi_i$ per ogni $i \in I$.

19. Una successione di sistemi diretti e di omomorfismi

    $$\mathbf{M} \to \mathbf{N} \to \mathbf{P}$$

    è *esatta* se la corrispondente successione di moduli e di omomorfismi di moduli è esatta per ogni $i \in I$. Provare che la successione $M \to N \to P$ di limiti diretti è allora esatta. [Usare l'Esercizio 15.]

I prodotti tensoriali commutano con i limiti diretti

20. Conservando le stesse notazioni dell'Esercizio 14, sia N un A-modulo arbitrario. Allora $(M_i \otimes N, \mu_{ij} \otimes 1)$ è un sistema diretto; sia $P = \varinjlim (M_i \otimes N)$ il suo limite diretto. Per ogni $i \in I$ si ha un omomorfismo $\mu_i \otimes 1: M_i \otimes N \to M \otimes N$, da cui, stante l'Esercizio 16, si ottiene un omomorfismo $\psi: P \to M \otimes N$. Pro-

vare che ψ è un isomorfismo, cosicché

$$\varinjlim (M_i \otimes N) \cong (\varinjlim M_i) \otimes N.$$

[Per ogni $i \in I$, sia $g_i \colon M_i \times N \to M_i \otimes N$ l'applicazione bilineare canonica. Passando al limite si ottiene un'applicazione $g \colon M \times \times N \to P$. Provare che g è A-bilineare e quindi definisce un omomorfismo $\phi \colon M \otimes N \to P$. Verificare che $\phi \circ \psi$ e $\psi \circ \phi$ sono applicazioni identiche.]

21. Sia $(A_i)_{i \in I}$ una famiglia di anelli indiciata da un insieme diretto I, e per ogni coppia di indici $i \leqslant j$ in I sia $\alpha_{ij} \colon A_i \to A_j$ un omomorfismo di anelli, soddisfacente alle condizioni (1) e (2) dell'Esercizio 14. Considerando ciascun A_i come uno Z-modulo, possiamo formare allora il limite diretto $A = \varinjlim A_i$. Dimostrare che A eredita una struttura di anello dagli A_i di modo che le applicazioni $A_i \to A$ sono omomorfismi di anelli. L'anello A è il *limite diretto* del sistema (A_i, α_{ij}).

    Se $A = 0$, provare che $A_i = 0$ per qualche $i \in I$. [Ricordare che tutti gli anelli hanno un elemento unità!]

22. Sia (A_i, α_{ij}) un sistema diretto di anelli e sia $\mathfrak{N}_i$ il nilradicale di A_i. Provare che il $\varinjlim \mathfrak{N}_i$ è il nilradicale di $\varinjlim A_i$.

    Se ciascun A_i è un dominio di integrità, allora $\varinjlim A_i$ è un dominio di integrità.

23. Sia $(B_\lambda)_{\lambda \in \Lambda}$ una famiglia di A-algebre. Per ogni sottoinsieme finito J di Λ denotiamo con B_J il prodotto tensoriale (sopra A) delle B_λ per $\lambda \in J$. Se J' è un altro sottoinsieme finito di Λ e $J \subseteq J'$, allora esiste un omomorfismo canonico di A-algebre $B_J \to B_{J'}$. Denotiamo con B il limite diretto degli anelli B_J al variare di J tra tutti i sottoinsiemi finiti di Λ. L'anello B possiede una struttura naturale di A-algebra rispetto alla quale gli omomorfismi $B_J \to \to B$ sono omomorfismi di A-algebre. La A-algebra B è il *prodotto tensoriale* della famiglia $(B_\lambda)_{\lambda \in \Lambda}$.

Piattezza e Tor

In questi Esercizi si supporrà che il lettore conosca la definizione e le proprietà fondamentali del funtore Tor.

24. Se M è un A-modulo, le seguenti condizioni sono equivalenti:
    i) M è piatto;

ii) $\mathrm{Tor}_n^A(M, N) = 0$ per ogni $n > 0$ e per ogni A-modulo N;

iii) $\mathrm{Tor}_1^A(M, N) = 0$ per ogni A-modulo N.

[Per dimostrare che (i) $\Rightarrow$ (ii), prendiamo una risoluzione libera di N e tensorizziamola con M. Poiché M è piatto, la successione così ottenuta è esatta e pertanto i suoi gruppi di omologia, che sono i $\mathrm{Tor}_n^A(M, N)$, sono nulli per $n > 0$. Per dimostrare che (iii) $\Rightarrow$ (i), consideriamo una successione esatta $0 \to N' \to N \to \to N'' \to 0$. Allora, dalla successione esatta dei Tor, si ha che la successione

$$\mathrm{Tor}_1(M, N'') \to M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$$

è esatta. Poiché $\mathrm{Tor}_1(M, N'') = 0$, ne segue che M è piatto.]

25. Sia $0 \to N' \to N \to N'' \to 0$ una successione esatta di A-moduli, con N'' piatto. Allora N' è piatto $\Leftrightarrow$ N è piatto. [Usare l'Esercizio 24 e la successione esatta dei Tor.]

26. Sia N un A-modulo. Allora N è piatto $\Leftrightarrow$ $\mathrm{Tor}_1(A/\mathfrak{a}, N) = 0$ per ogni ideale finitamente generato $\mathfrak{a}$ di A.
[Provare innanzitutto che N è piatto se $\mathrm{Tor}_1(M, N) = 0$ per ogni A-modulo *finitamente generato* M, usando (2.19). Se M è finitamente generato, siano $x_1, \ldots, x_n$ un sistema di generatori di M, e sia M_i il sottomodulo generato da $x_1, \ldots, x_i$. Considerando i quozienti successivi M_i/M_{i-1} e usando l'Esercizio 25, dedurre che N è piatto se $\mathrm{Tor}_1(M, N) = 0$ per ogni A-modulo *ciclico* M, ossia, per ogni A-modulo M generato da un solo elemento, e quindi della forma $A/\mathfrak{a}$ per qualche ideale $\mathfrak{a}$. Infine usare ancora (2.19) per ridursi al caso in cui $\mathfrak{a}$ è un ideale finitamente generato.]

27. Un anello A è *assolutamente piatto* se ogni A-modulo è piatto. Dimostrare che le seguenti condizioni sono equivalenti:

i) A è assolutamente piatto.

ii) Ogni ideale principale è idempotente.

iii) Ogni ideale finitamente generato è un addendo diretto di A.

[i) $\Rightarrow$ ii). Sia x un elemento di A. Allora $A/(x)$ è un A-modulo piatto, sicché nel diagramma

$$\begin{tikzcd}
(x) \otimes A \arrow[r, "\beta"] \arrow[d] & (x) \otimes A/(x) \arrow[d, "\alpha"] \\
A \arrow[r] & A/(x)
\end{tikzcd}$$

l'applicazione α è iniettiva. Dunque Im $(\beta) = 0$, da cui $(x) = (x^2)$. ii) $\Rightarrow$ iii). Sia $x \in A$. Allora $x = ax^2$ per qualche $a \in A$, sicché $e = ax$ è idempotente e si ha $(e) = (x)$. Ora se e, f sono idempotenti, si ha $(e, f) = (e + f - ef)$. Ne segue che ogni ideale finitamente generato è principale, e generato da un idempotente e; dunque è un addendo diretto poiché $A = (e) \oplus (1 - e)$. iii) $\Rightarrow$ i). [Usare il criterio dell'Esercizio 26.]

28. Un anello booleano è assolutamente piatto. L'anello considerato nell'Esercizio 7 del Capitolo 1 è assolutamente piatto. Ogni immagine omomorfa di un anello assolutamente piatto è un anello assolutamente piatto. Se un anello locale è assolutamente piatto, allora risulta un campo.

    Se A è assolutamente piatto, ogni elemento non invertibile in A è un divisore dello zero.

Capitolo terzo

Anelli e moduli di frazioni

La formazione degli anelli di frazioni e il procedimento di localizzazione ad essa associato sono forse gli strumenti tecnici più importanti in algebra commutativa. Il loro significato, nel linguaggio algebro-geometrico, consiste nel concentrare l'attenzione su un aperto o nell'intorno di un punto, e l'importanza di tali nozioni dovrebbe essere evidente di per sé. Questo capitolo dà le definizioni e le prime proprietà della formazione delle frazioni.

Il procedimento col quale si costruisce il campo razionale **Q** a partire dall'anello degli interi **Z** (e si immerge **Z** in **Q**) si estende facilmente ad un qualsiasi dominio di integrità A e dà luogo al *campo delle frazioni* (o *campo dei quozienti*) di A. La costruzione consiste nel prendere tutte le coppie ordinate (a, s) dove $a, s \in A$ e $s \neq 0$, e nell'introdurre una relazione di equivalenza tra tali coppie:

$$(a, s) \equiv (b, t) \Leftrightarrow at - bs = 0.$$

Ciò va bene soltanto se A è un dominio di integrità, poiché la verifica che la relazione è transitiva sfrutta la legge di cancellazione, ossia il fatto che A non possiede divisori dello zero $\neq 0$. Tuttavia, ciò può venire generalizzato nel modo seguente:

Sia A un anello arbitrario. Un *sottoinsieme moltiplicativamente chiuso* di A, o più brevemente, una *parte moltiplicativa* di A, è un sottoinsieme S di A tale che $1 \in S$ e S è chiuso rispetto alla moltiplicazione: in altre parole, S è un sotto-semigruppo del semigruppo moltiplicativo di A. Definiamo una relazione $\equiv$ su $A \times S$ nel modo seguente:

$$(a, s) \equiv (b, t) \Leftrightarrow (at - bs)u = 0 \text{ per qualche } u \in S.$$

Chiaramente tale relazione è riflessiva e simmetrica. Per provare che essa è transitiva, supponiamo che $(a, s) \equiv (b, t)$ e $(b, t) \equiv (c, u)$. Allora esistono elementi v, w in S tali che $(at - bs)v = 0$ e $(bu - ct)w =$

$= 0$. Eliminando b da queste due equazioni si ottiene: $(au - cs)tvw = 0$. Poiché S è chiuso rispetto alla moltiplicazione, si ha $tvw \in S$, da cui $(a, s) \equiv (c, u)$. Dunque si ha una relazione di equivalenza. Denotiamo con a/s la classe di equivalenza di (a, s), e con $S^{-1}A$ l'insieme delle classi di equivalenza. Costruiamo una struttura di anello su $S^{-1}A$ introducendo l'addizione e la moltiplicazione di tali "frazioni" a/s con le stesse definizioni usate in algebra elementare, ossia:

$$(a/s) + (b/t) = (at + bs)/st,$$
$$(a/s)(b/t) = ab/st.$$

Esercizio. *Verificare che tali definizioni sono indipendenti dalla scelta dei rappresentanti* (a, s) *e* (b, t), *e che* $S^{-1}A$ *soddisfa gli assiomi di un anello commutativo con unità.*

Si ha inoltre un omomorfismo di anelli $f: A \to S^{-1}A$ definito ponendo $f(x) = x/1$. Esso *non* è iniettivo in generale.

Osservazione. Se A è un dominio di integrità e $S = A - \{0\}$, allora $S^{-1}A$ è il campo delle frazioni di A.

L'anello $S^{-1}A$ è chiamato l'*anello delle frazioni* di A rispetto a S. Esso possiede una *proprietà universale:*

Proposizione 3.1. *Sia* $g: A \to B$ *un omomorfismo di anelli tale che* $g(s)$ *è invertibile in* B *per ogni* $s \in S$. *Allora esiste un unico omomorfismo di anelli* $h: S^{-1}A \to B$ *tale che* $g = h \circ f$.

Dimostrazione. i) *Unicità.* Se h soddisfa le condizioni richieste, allora $h(a/1) = hf(a) = g(a)$ per ogni $a \in A$; dunque, se $s \in S$,

$$h(1/s) = h((s/1)^{-1}) \stackrel{!}{=} h(s/1)^{-1} = g(s)^{-1}$$

e pertanto $h(a/s) = h(a/1) \quad h(1/s) = g(a)g(s)^{-1}$, sicché h è univocamente determinato da g.

ii) *Esistenza.* Poniamo $h(a/s) = g(a)g(s)^{-1}$. Allora h risulterà chiaramente un omomorfismo di anelli purché sia ben definito. Supponiamo dunque che $a/s = a'/s'$; allora esiste un elemento $t \in S$ tale che $(as' - a's)t = 0$, da cui

$$(g(a)g(s') - g(a')g(s))g(t) = 0;$$

ora $g(t)$ è invertibile in B, sicché $g(a)g(s)^{-1} = g(a')g(s')^{-1}$. ∎

L'anello $S^{-1}A$ e l'omomorfismo $f\colon A \to S^{-1}A$ possiedono le seguenti proprietà:

1) $s \in S \Rightarrow f(s)$ è invertibile in $S^{-1}A$;

2) $f(a) = 0 \Rightarrow as = 0$ per qualche $s \in S$;

3) Ogni elemento di $S^{-1}A$ è della forma $f(a)f(s)^{-1}$ per qualche $a \in A$ e qualche $s \in S$.

Viceversa, queste tre condizioni individuano l'anello $S^{-1}A$ a meno di isomorfismi. Precisamente:

Corollario 3.2. *Sia $g\colon A \to B$ un omomorfismo di anelli tale che:*

i) *$s \in S \Rightarrow g(s)$ è invertibile in B;*

ii) *$g(a) = 0 \Rightarrow as = 0$ per qualche $s \in S$;*

iii) *Ogni elemento di B è della forma $g(a)g(s)^{-1}$.*

Allora esiste un unico isomorfismo $h\colon S^{-1}A \to B$ tale che $g = h \circ f$.

Dimostrazione. In virtú di (3.1) occorre provare che $h\colon S^{-1}A \to B$, definito ponendo

$$h(a/s) = g(a)g(s)^{-1}$$

(tale definizione usa i)) è un isomorfismo. Stante iii), h è suriettivo. Per dimostrare che h è iniettivo, consideriamo il nucleo di h: se $h(a/s) = 0$, allora $g(a) = 0$, sicché, in virtú di ii), si ha $at = 0$ per qualche $t \in S$, e quindi $(a, s) \equiv (0, 1)$, ossia, $a/s = 0$ in $S^{-1}A$. ∎

Esempi. 1) Sia $\mathfrak{p}$ un ideale primo di A. Allora $S = A - \mathfrak{p}$ è una parte moltiplicativa (infatti $A - \mathfrak{p}$ è una parte moltiplicativa $\Leftrightarrow \mathfrak{p}$ è primo). Scriviamo in tal caso $A_\mathfrak{p}$ in luogo di $S^{-1}A$. Gli elementi a/s con $a \in \mathfrak{p}$ formano un ideale $\mathfrak{m}$ in $A_\mathfrak{p}$. Se $b/t \notin \mathfrak{m}$, allora $b \notin \mathfrak{p}$, sicché $b \in S$ e pertanto b/t è invertibile in $A_\mathfrak{p}$. Ne segue che se $\mathfrak{a}$ è un ideale in $A_\mathfrak{p}$ e $\mathfrak{a} \nsubseteq \mathfrak{m}$, allora $\mathfrak{a}$ contiene un elemento invertibile e pertanto è l'intero anello. Dunque $\mathfrak{m}$ è l'unico ideale massimale in $A_\mathfrak{p}$; in altre parole, $A_\mathfrak{p}$ è un *anello locale*.

Il procedimento di passaggio da A ad $A_\mathfrak{p}$ prende il nome di *localizzazione* in $\mathfrak{p}$.

2) $S^{-1}A$ è l'anello nullo $\Leftrightarrow 0 \in S$.

3) Sia $f \in A$ e $S = \{f^n\}_{n \geq 0}$. Scriviamo in tal caso A_f in luogo di $S^{-1}A$.

4) Sia $\mathfrak{a}$ un ideale qualsiasi di A, e poniamo $S = 1 + \mathfrak{a} =$ insieme di tutti gli elementi di A della forma $1 + x$ dove $x \in \mathfrak{a}$. Chiaramente S è una parte moltiplicativa.

5) Casi particolari di 1) e 3):

i) $A = \mathbf{Z}$, $\mathfrak{p} = (p)$, con p numero primo; $A_{\mathfrak{p}}$ = insieme di tutti i numeri razionali m/n dove n è primo rispetto a p; se $f \in \mathbf{Z}$ e $f \neq 0$, allora A_f è l'insieme di tutti i numeri razionali il cui denominatore è una potenza di f.

ii) $A = k[t_1, \ldots, t_n]$, dove k è un campo e le t_i sono indeterminate indipendenti, e $\mathfrak{p}$ è un ideale primo di A. Allora $A_{\mathfrak{p}}$ è l'anello di tutte le funzioni razionali f/g, dove $g \notin \mathfrak{p}$. Se V è la varietà definita dall'ideale $\mathfrak{p}$, ossia l'insieme di tutti gli $x = (x_1, \ldots, x_n) \in k^n$ tali che $f(x) = 0$ per ogni $f \in \mathfrak{p}$, allora (purché k sia infinito) $A_{\mathfrak{p}}$ può venire identificato con l'anello di tutte le funzioni razionali su k^n che sono definite in quasi tutti i punti di V; esso è l'anello locale di k^n *lungo la varietà* V. Tale anello è il prototipo degli anelli locali che si presentano in geometria algebrica.

La costruzione di $S^{-1}A$ può essere effettuata con un A-modulo M al posto dell'anello A. Definiamo una relazione $\equiv$ su $M \times S$ nel modo seguente:

$$(m, s) \equiv (m', s') \Leftrightarrow \exists t \in S \text{ tale che } t(sm' - s'm) = 0.$$

Come prima, si tratta di una relazione di equivalenza. Denotiamo con m/s la classe di equivalenza della coppia (m, s) e con $S^{-1}M$ l'insieme di tali frazioni, e introduciamo in $S^{-1}M$ una struttura di $S^{-1}A$-modulo con le ovvie definizioni di addizione e di moltiplicazione scalare. Come negli esempi 1) e 3) di cui sopra, scriviamo $M_{\mathfrak{p}}$ in luogo di $S^{-1}M$ quando $S = A - \mathfrak{p}$ ($\mathfrak{p}$ primo) e M_f quando $S = \{f^n\}_{n \geq 0}$.

Sia $u: M \to N$ un omomorfismo di A-moduli. Allora esso dà origine ad un omomorfismo di $S^{-1}A$-moduli $S^{-1}u: S^{-1}M \to S^{-1}N$, precisamente $S^{-1}u$ manda m/s in $u(m)/s$. Si ha inoltre $S^{-1}(v \circ u) = (S^{-1}v) \circ (S^{-1}u)$.

Proposizione 3.3. *L'operazione S^{-1} è esatta, ossia, se la successione $M' \xrightarrow{f} M \xrightarrow{g} M''$ è esatta in M, allora la successione $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ è esatta in $S^{-1}M$.*

Dimostrazione. Si ha $g \circ f = 0$, da cui $S^{-1}g \circ S^{-1}f = S^{-1}(0) = 0$, dunque $\operatorname{Im}(S^{-1}f) \subseteq \operatorname{Ker}(S^{-1}g)$. Per provare l'inclusione opposta, sia $m/s \in \operatorname{Ker}(S^{-1}g)$, allora $g(m)/s = 0$ in $S^{-1}M''$, dunque esiste un elemento $t \in S$ tale che $tg(m) = 0$ in M''. Ma $tg(m) = g(tm)$ poiché g è un omomorfismo di A-moduli, sicché $tm \in \operatorname{Ker}(g) = \operatorname{Im}(f)$ e pertanto $tm = f(m')$ per qualche $m' \in M'$. Dunque in $S^{-1}M$ si ha $m/s =$

$= f(m')/st = (S^{-1}f)(m'/st) \in \operatorname{Im}(S^{-1}f)$. Ne segue che $\operatorname{Ker}(S^{-1}g) \subseteq$ $\subseteq \operatorname{Im}(S^{-1}f)$. ■

In particolare, da (3.3) segue che se M' è un sottomodulo di M, l'applicazione $S^{-1}M' \to S^{-1}M$ è *iniettiva* e pertanto $S^{-1}M'$ può essere considerato come un sottomodulo di $S^{-1}M$. Con questa convenzione:

Corollario 3.4. *La formazione delle frazioni commuta con la formazione delle somme finite, delle intersezioni finite e dei quozienti. Precisamente, se N, P sono sottomoduli di un A-modulo M, allora*

i) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$

ii) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$

iii) *gli $S^{-1}A$-moduli $S^{-1}(M/N)$ e $(S^{-1}M)/(S^{-1}N)$ sono isomorfi.*

Dimostrazione. i) segue subito dalle definizioni e ii) è facile da verificare: se $y/s = z/t$ ($y \in N$, $z \in P$, $s, t \in S$) allora $u(ty - sz) = 0$ per qualche $u \in S$, sicché $w = uty = usz \in N \cap P$ e pertanto $y/s =$ $= w/stu \in S^{-1}(N \cap P)$. Ne segue che $S^{-1}N \cap S^{-1}P \subseteq S^{-1}(N \cap P)$, e l'inclusione opposta è ovvia.

iii) Basta applicare S^{-1} alla successione esatta $0 \to N \to M \to$ $\to M/N \to 0$. ■

Proposizione 3.5. *Sia M un A-modulo. Allora gli $S^{-1}A$-moduli $S^{-1}M$ e $S^{-1}A \otimes_A M$ sono isomorfi; più precisamente, esiste un unico isomorfismo $f\colon S^{-1}A \otimes_A M \to S^{-1}M$ per il quale*

(1) $\qquad f((a/s) \otimes m) = am/s$ *per ogni* $a \in A, m \in M, s \in S$.

Dimostrazione. L'applicazione $S^{-1}A \times M \to S^{-1}M$ definita da

$$(a/s, m) \mapsto am/s$$

è A-bilineare, e pertanto per la proprietà universale (2.12) del prodotto tensoriale induce un A-omomorfismo

$$f\colon S^{-1}A \otimes_A M \to S^{-1}M$$

che soddisfa la (1). Chiaramente f è suriettivo, ed è univocamente definito dalla (1).

Sia $\sum_i (a_i/s_i) \otimes m_i$ un elemento arbitrario di $S^{-1}A \otimes M$. Se $s =$ $= \prod_i s_i \in S$, $t_i = \prod_{j \neq i} s_j$, si ha

$$\sum_i \frac{a_i}{s_i} \otimes m_i = \sum_i \frac{a_i t_i}{s} \otimes m = \sum_i \frac{1}{s} \otimes a_i t_i m = \frac{1}{s} \otimes \sum_i a_i t_i m,$$

sicché ogni elemento di $S^{-1}A \otimes M$ è della forma $(1/s) \otimes m$. Supponiamo che $f((1/s) \otimes m) = 0$. Allora $m/s = 0$, da cui $tm = 0$ per qualche $t \in S$, e pertanto

$$\frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0.$$

Dunque f è iniettivo e pertanto è un isomorfismo. ∎

Corollario 3.6. *$S^{-1}A$ è un A-modulo piatto.*

Dimostrazione. Utilizzare (3.3) e (3.5). ∎

Proposizione 3.7. *Se M, N sono A-moduli, vi è un unico isomorfismo di $S^{-1}A$-moduli $f\colon S^{-1}M \otimes_{S^{-1}A} S^{-1}N \to S^{-1}(M \otimes_A N)$ tale che*

$$f((m/s) \otimes (n/t)) = (m \otimes n)/st.$$

In particolare, se $\mathfrak{p}$ è un ideale primo arbitrario, allora

$$M_\mathfrak{p} \otimes_{A_\mathfrak{p}} N_\mathfrak{p} = (M \otimes_A N)_\mathfrak{p}$$

come $A_\mathfrak{p}$-moduli.

Dimostrazione. Utilizzare (3.5) e gli isomorfismi canonici del Capitolo 2. ∎

Proprietà locali

Una proprietà P di un anello A (o di un A-modulo M) si dice una *proprietà locale*, se vale la seguente condizione:

A (risp. M) possiede la proprietà $P \Leftrightarrow A_\mathfrak{p}$ (risp. $M_\mathfrak{p}$) possiede la proprietà P, per ogni ideale primo $\mathfrak{p}$ di A. Le proposizioni seguenti forniscono esempi di proprietà locali:

Proposizione 3.8. *Sia M un A-modulo. Allora le seguenti condizioni sono equivalenti:*

i) $M = 0$;

ii) $M_\mathfrak{p} = 0$ *per ogni ideale primo $\mathfrak{p}$ di A;*

iii) $M_\mathfrak{m} = 0$ *per ogni ideale massimale $\mathfrak{m}$ di A.*

Dimostrazione. Chiaramente i) $\Rightarrow$ ii) $\Rightarrow$ iii). Supponiamo che la iii) sia soddisfatta e $M \neq 0$. Sia x un elemento non nullo di M, e poniamo $\mathfrak{a} = \operatorname{Ann}(x)$; $\mathfrak{a}$ è un ideale $\neq (1)$, dunque è contenuto in un ideale massimale $\mathfrak{m}$, in virtú di (1.4). Consideriamo l'elemento $x/1 \in M_{\mathfrak{m}}$. Poiché $M_{\mathfrak{m}} = 0$ si ha $x/1 = 0$, sicché x è annullato da qualche elemento di $A - \mathfrak{m}$; ma ciò è impossibile poiché $\mathrm{Ann}(x) \subseteq \mathfrak{m}$. ■

Proposizione 3.9. *Sia $\phi: M \to N$ un omomorfismo di A-moduli. Allora le seguenti condizioni sono equivalenti:*

i) *ϕ è iniettivo;*

ii) *$\phi_{\mathfrak{p}}: M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ è iniettivo per ogni ideale primo $\mathfrak{p}$;*

iii) *$\phi_{\mathfrak{m}}: M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ è iniettivo per ogni ideale massimale $\mathfrak{m}$.*

Vale un risultato simile sostituendo ovunque "iniettivo" con "suriettivo".

Dimostrazione. i) $\Rightarrow$ ii). $0 \to M \to N$ è una successione esatta, quindi $0 \to M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ è esatta, ossia, $\phi_{\mathfrak{p}}$ è iniettivo.

ii) $\Rightarrow$ iii) giacché un ideale massimale è primo.

iii) $\Rightarrow$ i). Posto $M' = \mathrm{Ker}(\phi)$, la successione $0 \to M' \to M \to N$ è esatta, quindi $0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ è esatta, in virtú di (3.3), e pertanto $M'_{\mathfrak{m}} \cong \mathrm{Ker}(\phi_{\mathfrak{m}}) = 0$ poiché $\phi_{\mathfrak{m}}$ è iniettivo. Ne segue, stante (3.8), che $M' = 0$, dunque ϕ è iniettivo.

Per ottenere l'altra parte della proposizione, basta invertire tutte le frecce. ■

La piattezza è una proprietà locale:

Proposizione 3.10. *Per un qualsiasi A-modulo M, le seguenti affermazioni sono equivalenti:*

i) *M è un A-modulo piatto;*

ii) *$M_{\mathfrak{p}}$ è un $A_{\mathfrak{p}}$-modulo piatto per ogni ideale primo $\mathfrak{p}$;*

iii) *$M_{\mathfrak{m}}$ è un $A_{\mathfrak{m}}$-modulo piatto per ogni ideale massimale $\mathfrak{m}$.*

Dimostrazione. i) $\Rightarrow$ ii) segue da (3.5) e (2.20).

ii) $\Rightarrow$ iii) è immediato.

iii) $\Rightarrow$ i). Se $N \to P$ è un omomorfismo di A-moduli, e $\mathfrak{m}$ è un arbitrario ideale massimale di A, allora

$$
\begin{aligned}
N \to P \text{ iniettivo} &\Rightarrow N_{\mathfrak{m}} \to P_{\mathfrak{m}} \text{ iniettivo, in virtú di (3.9)} \\
&\Rightarrow N_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \to P_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} M_{\mathfrak{m}} \text{ iniettivo, in virtú di (2.19)} \\
&\Rightarrow (N \otimes_A M)_{\mathfrak{m}} \to (P \otimes_A M)_{\mathfrak{m}} \text{ iniettivo, in virtú di (3.7)} \\
&\Rightarrow N \otimes_A M \to P \otimes_A M \text{ iniettivo, in virtú di (3.9).}
\end{aligned}
$$

Ne segue, stante (2.19), che M è piatto. ■

Ideali estesi e contratti negli anelli di frazioni

Sia A un anello, S una parte moltiplicativa di A e $f: A \to S^{-1}A$ l'omomorfismo naturale, definito ponendo $f(a) = a/1$. Sia C l'insieme degli ideali contratti in A, e sia E l'insieme degli ideali estesi in $S^{-1}A$ (cfr. (1.17)). Se $\mathfrak{a}$ è un ideale in A, la sua estensione $\mathfrak{a}^e$ in $S^{-1}A$ è $S^{-1}\mathfrak{a}$ (infatti un qualsiasi elemento $y \in \mathfrak{a}^e$ è della forma $\sum a_i/s_i$, dove $a_i \in \mathfrak{a}$ e $s_i \in S$, sicché basta prendere un comune denominatore).

Proposizione 3.11. i) *Ogni ideale in $S^{-1}A$ è un ideale esteso.*

ii) *Se $\mathfrak{a}$ è un ideale in A, allora $\mathfrak{a}^{ec} = \bigcup_{s \in S}(\mathfrak{a}: s)$. Dunque $\mathfrak{a}^e = (1)$ se, e soltanto se, $\mathfrak{a}$ incontra S.*

iii) *$\mathfrak{a} \in C \Leftrightarrow$ nessun elemento di S è un divisore dello zero in $A/\mathfrak{a}$.*

iv) *Gli ideali primi di $S^{-1}A$ sono in corrispondenza biunivoca ($\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$) con gli ideali primi di A che non incontrano S.*

v) *L'operazione S^{-1} commuta con la formazione di somme finite, prodotti finiti, intersezioni finite e del radicale.*

Dimostrazione. i) Sia $\mathfrak{b}$ un ideale in $S^{-1}A$, e sia $x/s \in \mathfrak{b}$. Allora $x/1 \in \mathfrak{b}$, dunque $x \in \mathfrak{b}^c$ e pertanto $x/s \in \mathfrak{b}^{ce}$. Poiché $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$ in ogni caso (1.17), ne segue che $\mathfrak{b} = \mathfrak{b}^{ce}$.

ii) $x \in \mathfrak{a}^{ec} = (S^{-1}\mathfrak{a})^c \Leftrightarrow x/1 = a/s$ per qualche $a \in \mathfrak{a}$, $s \in S \Leftrightarrow (xs - a)t = 0$ per qualche $t \in S \Leftrightarrow xst \in \mathfrak{a} \Leftrightarrow x \in \bigcup_{s \in S}(\mathfrak{a}: s)$.

iii) $\mathfrak{a} \in C \Leftrightarrow \mathfrak{a}^{ec} \subseteq \mathfrak{a} \Leftrightarrow (sx \in \mathfrak{a}$ per qualche $s \in S \Rightarrow x \in \mathfrak{a}) \Leftrightarrow$ nessun elemento $s \in S$ è un divisore dello zero in $A/\mathfrak{a}$.

iv) Se $\mathfrak{q}$ è un ideale primo di $S^{-1}A$, allora $\mathfrak{q}^c$ è un ideale primo in A (ciò è vero per un qualsiasi omomorfismo di anelli). Viceversa, se $\mathfrak{p}$ è un ideale primo in A, allora $A/\mathfrak{p}$ è un dominio di integrità; se $\bar{S}$ è l'immagine di S in $A/\mathfrak{p}$, si ha: $S^{-1}A/S^{-1}\mathfrak{p} \cong \bar{S}^{-1}(A/\mathfrak{p})$, il quale o è l'anello nullo oppure è contenuto nel campo delle frazioni di $A/\mathfrak{p}$ ed è pertanto un dominio di integrità, e quindi $S^{-1}\mathfrak{p}$ è primo oppure è l'ideale unità; in virtú di ii), la seconda eventualità si verifica se, e soltanto se, $\mathfrak{p}$ incontra S.

v) Per somme e prodotti, la tesi segue da (1.18); per le intersezioni, da (3.4). Per quanto riguarda i radicali, si ha $S^{-1}r(\mathfrak{a}) \subseteq r(S^{-1}\mathfrak{a})$, in virtú di (1.18), e la dimostrazione dell'inclusione opposta è una semplice verifica che lasciamo al lettore. ■

Osservazioni. 1) Se $\mathfrak{a}, \mathfrak{b}$ sono ideali di A, la formula

$$S^{-1}(\mathfrak{a}:\mathfrak{b}) = (S^{-1}\mathfrak{a}:S^{-1}\mathfrak{b})$$

è valida purché l'ideale $\mathfrak{b}$ sia finitamente generato: cfr. (3.15).

2) La dimostrazione data in (1.8) del fatto che, se $f \in A$ non è nilpotente, vi è un ideale primo di A che non contiene f, può essere espressa in modo piú conciso nel linguaggio degli anelli di frazioni. Poiché l'insieme $S = \{f^n\}_{n \geq 0}$ non contiene lo zero, l'anello $S^{-1}A = A_f$ non è l'anello nullo e pertanto, stante (1.3), possiede un ideale massimale, la cui contrazione in A è un ideale primo $\mathfrak{p}$ che non incontra S, in virtú di (3.11); dunque $f \notin \mathfrak{p}$.

Corollario 3.12. *Se $\mathfrak{N}$ è il nilradicale di A, il nilradicale di $S^{-1}A$ è $S^{-1}\mathfrak{N}$.* ∎

Corollario 3.13. *Se $\mathfrak{p}$ è un ideale primo di A, gli ideali primi dell'anello locale $A_\mathfrak{p}$ sono in corrispondenza biunivoca con gli ideali primi di A contenuti in $\mathfrak{p}$.*

Dimostrazione. Basta prendere $S = A - \mathfrak{p}$ in (3.11) (iv). ∎

Osservazione. Dunque il passaggio da A ad $A_\mathfrak{p}$ fa sparire tutti gli ideali primi tranne quelli contenuti in $\mathfrak{p}$. Nell'altra direzione, il passaggio da A ad $A/\mathfrak{p}$ fa sparire tutti gli ideali primi tranne quelli contenenti $\mathfrak{p}$. Ne segue che se $\mathfrak{p}$, $\mathfrak{q}$ sono ideali primi tali che $\mathfrak{p} \supseteq \mathfrak{q}$, allora localizzando rispetto a $\mathfrak{p}$ e prendendo il quoziente mod $\mathfrak{q}$ (in un ordine qualsiasi: queste due operazioni commutano, in virtú di (3.4)), si restringe l'attenzione a quegli ideali primi che si trovano tra $\mathfrak{p}$ e $\mathfrak{q}$. In particolare, se $\mathfrak{p} = \mathfrak{q}$, si perviene alla fine ad un campo, detto il *campo residuo in* $\mathfrak{p}$, il quale può essere ottenuto o come il campo delle frazioni del dominio di integrità $A/\mathfrak{p}$ oppure come il campo residuo dell'anello locale $A_\mathfrak{p}$.

Proposizione 3.14. *Sia M un A-modulo finitamente generato, S una parte moltiplicativa di A. Allora $S^{-1}(\mathrm{Ann}\,(M)) = \mathrm{Ann}\,(S^{-1}M)$.*

Dimostrazione. Se ciò è vero per due A-moduli M, N, è vero per $M + N$:

$$\begin{aligned} S^{-1}(\mathrm{Ann}\,(M+N)) &= S^{-1}(\mathrm{Ann}\,(M) \cap \mathrm{Ann}\,(N)) \text{ in virtú di (2.2)} \\ &= S^{-1}(\mathrm{Ann}\,(M)) \cap S^{-1}(\mathrm{Ann}\,(N)) \text{ in virtú di (3.4)} \\ &= \mathrm{Ann}\,(S^{-1}M) \cap \mathrm{Ann}\,(S^{-1}N) \text{ per ipotesi} \\ &= \mathrm{Ann}\,(S^{-1}M + S^{-1}N) = \mathrm{Ann}\,(S^{-1}(M+N)). \end{aligned}$$

Dunque basta provare (3.14) per un A-modulo M generato da un solo elemento: allora $M \cong A/\mathfrak{a}$ (come A-modulo), dove $\mathfrak{a} = \mathrm{Ann}(M)$; $S^{-1}M \cong (S^{-1}A)/(S^{-1}\mathfrak{a})$ in virtú di (3.4), sicché $\mathrm{Ann}(S^{-1}M) = S^{-1}\mathfrak{a} = S^{-1}(\mathrm{Ann}(M))$. ■

Corollario 3.15. *Se N, P sono sottomoduli di un A-modulo M e se P è finitamente generato, allora $S^{-1}(N:P) = (S^{-1}N:S^{-1}P)$.*

Dimostrazione. $(N:P) = \mathrm{Ann}((N+P)/N)$, stante (2.2); ora basta applicare (3.14). ■

Proposizione 3.16. *Sia dato un omomorfismo di anelli $A \to B$ e sia $\mathfrak{p}$ un ideale primo di A. Allora $\mathfrak{p}$ è la contrazione di un ideale primo di B se, e soltanto se, $\mathfrak{p}^{ec} = \mathfrak{p}$.*

Dimostrazione. Se $\mathfrak{p} = \mathfrak{q}^c$, allora $\mathfrak{p}^{ec} = \mathfrak{p}$ in virtú di (1.17). Viceversa, se $\mathfrak{p}^{ec} = \mathfrak{p}$, sia S l'immagine di $A - \mathfrak{p}$ in B. Allora $\mathfrak{p}^e$ non incontra S; pertanto, in virtú di (3.11), la sua estensione in $S^{-1}B$ è un ideale proprio e quindi è contenuta in un ideale massimale $\mathfrak{m}$ di $S^{-1}B$. Se $\mathfrak{q}$ è la contrazione di $\mathfrak{m}$ in B, allora $\mathfrak{q}$ è primo, $\mathfrak{q} \supseteq \mathfrak{p}^e$ e $\mathfrak{q} \cap S = \emptyset$. Dunque $\mathfrak{q}^c = \mathfrak{p}$. ■

Esercizi

1. Sia S una parte moltiplicativa di un anello A, e sia M un A-modulo finitamente generato. Provare che $S^{-1}M = 0$ se e soltanto se esiste un elemento $s \in S$ tale che $sM = 0$.
2. Sia $\mathfrak{a}$ un ideale di un anello A, e sia $S = 1 + \mathfrak{a}$. Dimostrare che $S^{-1}\mathfrak{a}$ è contenuto nel radicale di Jacobson di $S^{-1}A$.

   Utilizzare questo risultato e il lemma di Nakayama per dare una dimostrazione di (2.5) che non dipende dai determinanti. [Se $M = \mathfrak{a}M$, allora $S^{-1}M = (S^{-1}\mathfrak{a})(S^{-1}M)$, da cui, in virtú del lemma di Nakayama, si ha $S^{-1}M = 0$. Ora basta utilizzare l'Esercizio 1.]
3. Sia A un anello, siano S e T due parti moltiplicative di A, e sia U l'immagine di T in $S^{-1}A$. Dimostrare che gli anelli $(ST)^{-1}A$ e $U^{-1}(S^{-1}A)$ sono isomorfi.
4. Sia $f: A \to B$ un omomorfismo di anelli e sia S una parte moltiplicativa di A. Poniamo $T = f(S)$. Provare che $S^{-1}B$ e $T^{-1}B$ sono isomorfi come $S^{-1}A$-moduli.
5. Sia A un anello. Supponiamo che, per ogni ideale primo $\mathfrak{p}$, l'anello locale $A_\mathfrak{p}$ non abbia elementi nilpotenti $\neq 0$. Dimostrare che

A non possiede elementi nilpotenti $\neq 0$. Se ogni anello $A_\mathfrak{p}$ è un dominio di integrità, A risulta necessariamente un dominio di integrità?

6. Sia A un anello $\neq 0$ e sia Σ l'insieme di tutte le parti moltiplicative S di A tali che $0 \notin S$. Provare che Σ possiede elementi massimali, e che $S \in \Sigma$ è massimale se e soltanto se $A - S$ è un ideale primo minimale di A.

7. Una parte moltiplicativa S di un anello A si dice *saturata* se

$$xy \in S \Leftrightarrow x \in S \text{ e } y \in S.$$

Dimostrare che:

i) S è saturata $\Leftrightarrow A - S$ è un'unione di ideali primi.

ii) Se S è una qualsiasi parte moltiplicativa di A, vi è un'unica parte moltiplicativa saturata minima $\bar{S}$ contenente S e inoltre che $\bar{S}$ è il complementare in A dell'unione degli ideali primi che non incontrano S. ($\bar{S}$ è chiamata la *saturazione* di S.)

Se $S = 1 + \mathfrak{a}$, dove $\mathfrak{a}$ è un ideale di A, determinare $\bar{S}$.

8. Siano S, T parti moltiplicative di A, tali che $S \subseteq T$. Sia $\phi: S^{-1}A \to T^{-1}A$ l'omomorfismo che manda ciascun elemento $a/s \in S^{-1}A$ in a/s considerato come elemento di $T^{-1}A$. Dimostrare che le seguenti condizioni sono equivalenti:

i) ϕ è biiettivo.

ii) Per ogni $t \in T$, $t/1$ è invertibile in $S^{-1}A$.

iii) Per ogni $t \in T$, esiste un elemento $x \in A$ tale che $xt \in S$.

iv) T è contenuta nella saturazione di S (Esercizio 7).

v) Ogni ideale primo che incontra T incontra anche S.

9. L'insieme S_0 di tutti gli elementi che non sono divisori dello zero in A è una parte moltiplicativa saturata di A. Dunque l'insieme D dei divisori dello zero in A è un'unione di ideali primi (cfr. Capitolo 1, Esercizio 14). Provare che ogni ideale primo minimale di A è contenuto in D. [Utilizzare l'Esercizio 6.]

L'anello $S_0^{-1}A$ è chiamato l'*anello totale delle frazioni* di A. Dimostrare che:

i) S_0 è la più grande parte moltiplicativa di A per la quale l'omomorfismo $A \to S_0^{-1}A$ è iniettivo.

ii) Ogni elemento in $S_0^{-1}A$ o è un divisore dello zero oppure è invertibile.

iii) Ogni anello in cui ogni elemento non invertibile è un divisore dello zero coincide col suo anello totale delle frazioni (ossia, $A \to S_0^{-1}A$ è biiettivo).

10. Sia A un anello.

i) Se A è assolutamente piatto (Capitolo 2, Esercizio 27) e S è una parte moltiplicativa arbitraria di A, allora $S^{-1}A$ è assolutamente piatto.

ii) A è assolutamente piatto $\Leftrightarrow$ $A_{\mathfrak{m}}$ è un campo per ogni ideale massimale $\mathfrak{m}$.

11. Sia A un anello. Dimostrare che le seguenti condizioni sono equivalenti:

i) $A/\mathfrak{N}$ è assolutamente piatto (essendo $\mathfrak{N}$ il nilradicale di A).

ii) Ogni ideale primo di A è massimale.

iii) Spec (A) è uno spazio T_1 (ossia, ogni sottoinsieme costituito da un solo punto è chiuso).

iv) Spec (A) è uno spazio di Hausdorff.

Se queste condizioni sono soddisfatte, provare che Spec (A) è compatto e totalmente sconnesso (ossia, gli unici sottoinsiemi connessi di Spec (A) sono quelli costituiti da un solo punto).

12. Sia A un dominio di integrità e M un A-modulo. Un elemento $x \in M$ è un *elemento di torsione* di M se $\mathrm{Ann}(x) \neq 0$, ossia se x è annullato da qualche elemento non nullo di A. Dimostrare che gli elementi di torsione di M formano un sottomodulo di M. Tale sottomodulo è chiamato il *sottomodulo di torsione* di M e si denota con $T(M)$. Se $T(M) = 0$, si dice che il modulo M è privo di torsione. Provare che:

i) Se M è un A-modulo qualsiasi, $M/T(M)$ è privo di torsione.

ii) Se $f: M \to N$ è un omomorfismo di moduli, allora $f(T(M)) \subseteq T(N)$.

iii) Se $0 \to M' \to M \to M''$ è una successione esatta, allora la successione $0 \to T(M') \to T(M) \to T(M'')$ è esatta.

iv) Se M è un A-modulo qualsiasi, $T(M)$ è il nucleo dell'applicazione $x \mapsto 1 \otimes x$ di M in $K \otimes_A M$, dove K è il campo delle frazioni di A.

[Per ottenere iv), mostrare che K può essere considerato come il limite diretto dei suoi sottomoduli $A\xi$ ($\xi \in K$); utilizzando gli Esercizi 15 e 20 del Capitolo 1, provare che se $1 \otimes x = 0$ in

$K \otimes M$, allora $1 \otimes x = 0$ in $A\xi \otimes M$ per qualche $\xi \neq 0$. Dedurre che $\xi^{-1}x = 0$.]

13. Sia S una parte moltiplicativa di un dominio di integrità A. Con le notazioni dell'Esercizio 12, dimostrare che $T(S^{-1}M) = S^{-1}(T(M))$. Dedurre che le seguenti condizioni sono equivalenti:

    i) M è privo di torsione.
    ii) $M_\mathfrak{p}$ è privo di torsione per ogni ideale primo $\mathfrak{p}$.
    iii) $M_\mathfrak{m}$ è privo di torsione per ogni ideale massimale $\mathfrak{m}$.

14. Sia M un A-modulo e $\mathfrak{a}$ un ideale di A. Supponiamo che $M_\mathfrak{m} = 0$ per ogni ideale massimale $\mathfrak{m} \supseteq \mathfrak{a}$. Provare che $M = \mathfrak{a}M$. [Passare all'$A/\mathfrak{a}$-modulo $M/\mathfrak{a}M$ e utilizzare (3.8).]

15. Sia A un anello, e sia F l'A-modulo A^n. Dimostrare che ogni sistema di n generatori di F è una base di F. [Sia $x_1, \ldots, x_n$ un sistema di generatori ed $e_1, \ldots, e_n$ la base canonica di F. Definiamo $\phi: F \to F$ ponendo $\phi(e_i) = x_i$. Allora ϕ è suriettivo e occorre provare che esso è un isomorfismo. In virtù di (3.9), possiamo supporre che A è un anello locale. Sia N il nucleo di ϕ e sia $k = A/\mathfrak{m}$ il campo residuo di A. Poiché F è un A-modulo piatto, la successione esatta $0 \to N \to F \to F \to 0$ fornisce una successione esatta $0 \to k \otimes N \to k \otimes F \xrightarrow{1 \otimes \phi} k \otimes F \to 0$. Ora $k \otimes F = k^n$ è uno spazio vettoriale di dimensione n sopra k; $1 \otimes \phi$ è suriettivo, dunque biiettivo, e quindi $k \otimes N = 0$.

    Inoltre N è finitamente generato, in virtú dell'Esercizio 12 del Capitolo 2, e quindi $N = 0$, per il lemma di Nakayama. Dunque ϕ è un isomorfismo.]

    Dedurre che ogni sistema di generatori di F possiede almeno n elementi.

16. Sia B una A-algebra piatta. Allora le seguenti condizioni sono equivalenti:

    i) $\mathfrak{a}^{ec} = \mathfrak{a}$ per ogni ideale $\mathfrak{a}$ di A.
    ii) L'applicazione canonica Spec $(B) \to$ Spec (A) è suriettiva.
    iii) Per ogni ideale massimale $\mathfrak{m}$ di A si ha $\mathfrak{m}^e \neq (1)$.
    iv) Se M è un A-modulo non nullo qualsiasi, allora $M_B \neq 0$.
    v) Per ogni A-modulo M, l'applicazione $x \mapsto 1 \otimes x$ di M in M_B è iniettiva.

    [Per provare che i) $\Rightarrow$ ii), utilizzare (3.16). ii) $\Rightarrow$ iii) è chiaro.
    iii) $\Rightarrow$ iv): Sia x un elemento non nullo di M e poniamo $M' = Ax$. Poiché B è piatto sopra A, basta provare che $M'_B \neq 0$. Si ha

$M' \cong A/\mathfrak{a}$ per qualche ideale $\mathfrak{a} \neq (1)$, da cui $M'_B \cong B/\mathfrak{a}^e$. Ora $\mathfrak{a} \subseteq \mathfrak{m}$ per qualche ideale massimale $\mathfrak{m}$, sicché $\mathfrak{a}^e \subseteq \mathfrak{m}^e \neq (1)$. Dunque $M'_B \neq 0$.

iv) $\Rightarrow$ v): Sia M' il nucleo di $M \to M_B$. Poiché B è piatto sopra A, la successione $0 \to M'_B \to M_B \to (M_B)_B$ è esatta. Ebbene (utilizzando l'Esercizio 13 del Capitolo 2, con $N = M_B$) l'applicazione $M_B \to (M_B)_B$ è iniettiva, sicché $M'_B = 0$ e pertanto $M' = 0$.

v) $\Rightarrow$ i): Basta prendere $M = A/\mathfrak{a}$.]

Un anello B siffatto si dice *fedelmente piatto* sopra A.

17. Siano $A \xrightarrow{f} B \xrightarrow{g} C$ omomorfismi di anelli. Se $g \circ f$ è piatto e g è fedelmente piatto, allora f è piatto.

18. Sia f: $A \to B$ un omomorfismo piatto di anelli, sia $\mathfrak{q}$ un ideale primo di B e sia $\mathfrak{p} = \mathfrak{q}^c$. Allora f^*: $\operatorname{Spec}(B_\mathfrak{q}) \to \operatorname{Spec}(A_\mathfrak{p})$ è suriettiva. [Infatti $B_\mathfrak{p}$ è piatto sopra $A_\mathfrak{p}$ in virtú di (3.10), e $B_\mathfrak{q}$ è un anello locale di $B_\mathfrak{p}$, dunque è piatto sopra $B_\mathfrak{p}$. Ne segue che $B_\mathfrak{q}$ è piatto sopra $A_\mathfrak{p}$ e soddisfa la condizione (3) dell'Esercizio 16.]

19. Sia A un anello, M un A-modulo. Si definisce *supporto* di M l'insieme $\operatorname{Supp}(M)$ degli ideali primi $\mathfrak{p}$ di A tali che $M_\mathfrak{p} \neq 0$. Dimostrare i seguenti risultati:

   i) $M \neq 0 \Leftrightarrow \operatorname{Supp}(M) \neq \emptyset$.
   ii) $V(\mathfrak{a}) = \operatorname{Supp}(A/\mathfrak{a})$.
   iii) Se $0 \to M' \to M \to M'' \to 0$ è una successione esatta, allora $\operatorname{Supp}(M) = \operatorname{Supp}(M') \cup \operatorname{Supp}(M'')$.
   iv) Se $M = \sum M_i$, allora $\operatorname{Supp}(M) = \bigcup \operatorname{Supp}(M_i)$.
   v) Se M è finitamente generato, allora $\operatorname{Supp}(M) = V(\operatorname{Ann}(M))$ (ed è pertanto un sottoinsieme chiuso di $\operatorname{Spec}(A)$).
   vi) Se M, N sono finitamente generati, allora $\operatorname{Supp}(M \otimes_A N) = \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$. [Utilizzare l'Esercizio 3 del Capitolo 2.]
   vii) Se M è finitamente generato e $\mathfrak{a}$ è un ideale di A, allora $\operatorname{Supp}(M/\mathfrak{a}M) = V(\mathfrak{a} + \operatorname{Ann}(M))$.
   viii) Se f: $A \to B$ è un omomorfismo di anelli e M è un A-modulo finitamente generato, allora $\operatorname{Supp}(B \otimes_A M) = f^{*-1}(\operatorname{Supp}(M))$.

20. Sia f: $A \to B$ un omomorfismo di anelli, f^*: $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ l'applicazione associata. Dimostrare che:

   i) Ogni ideale primo di A è un ideale contratto $\Leftrightarrow f^*$ è suriettiva.

ii) Se ogni ideale primo di B è un ideale esteso, allora f^* è iniettiva. Vale il viceversa?

21. i) Sia A un anello, S una parte moltiplicativa di A e $\phi\colon A \to S^{-1}A$ l'omomorfismo canonico. Dimostrare che $\phi^*\colon \operatorname{Spec}(S^{-1}A) \to \operatorname{Spec}(A)$ è un omeomorfismo di $\operatorname{Spec}(S^{-1}A)$ sulla sua immagine in $X = \operatorname{Spec}(A)$. Denotiamo tale immagine con $S^{-1}X$.
In particolare, se $f \in A$, l'immagine di $\operatorname{Spec}(A_f)$ in X è l'aperto fondamentale X_f (Capitolo 1, Esercizio 17).

ii) Sia $f\colon A \to B$ un omomorfismo di anelli. Poniamo $X = \operatorname{Spec}(A)$ e $Y = \operatorname{Spec}(B)$, e sia $f^*\colon Y \to X$ l'applicazione associata a f. Identificando $\operatorname{Spec}(S^{-1}A)$ con la sua immagine canonica $S^{-1}X$ in X, e $\operatorname{Spec}(S^{-1}B)$ ($= \operatorname{Spec}(f(S)^{-1}B)$ con la sua immagine canonica $S^{-1}Y$ in Y, provare che $S^{-1}f^*\colon \operatorname{Spec}(S^{-1}B) \to \operatorname{Spec}(S^{-1}A)$ è la restrizione di f^* a $S^{-1}Y$, e che $S^{-1}Y = f^{*-1}(S^{-1}X)$.

iii) Sia $\mathfrak{a}$ un ideale di A e sia $\mathfrak{b} = \mathfrak{a}^e$ la sua estensione in B. Sia $\bar{f}\colon A/\mathfrak{a} \to B/\mathfrak{b}$ l'omomorfismo indotto da f. Se si identifica $\operatorname{Spec}(A/\mathfrak{a})$ con la sua immagine canonica $V(\mathfrak{a})$ in X, e $\operatorname{Spec}(B/\mathfrak{b})$ con la sua immagine canonica $V(\mathfrak{b})$ in Y, dimostrare che $\bar{f}^*$ è la restrizione di f^* a $V(\mathfrak{b})$.

iv) Sia $\mathfrak{p}$ un ideale primo di A. Prendiamo $S = A - \mathfrak{p}$ in ii) e successivamente riduciamo mod $S^{-1}\mathfrak{p}$ come in iii). Dedurre che il sottospazio $f^{*-1}(\mathfrak{p})$ di Y è omeomorfo in modo naturale a $\operatorname{Spec}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}) = \operatorname{Spec}(k(\mathfrak{p}) \otimes_A B)$, dove $k(\mathfrak{p})$ è il campo residuo dell'anello locale $A_\mathfrak{p}$.
$\operatorname{Spec}(k(\mathfrak{p}) \otimes_A B)$ prende il nome di *fibra* di f^* sopra $\mathfrak{p}$.

22. Sia A un anello e $\mathfrak{p}$ un ideale primo di A. Allora l'immagine canonica di $\operatorname{Spec}(A_\mathfrak{p})$ in $\operatorname{Spec}(A)$ è uguale all'intersezione di tutti gli intorni aperti di $\mathfrak{p}$ in $\operatorname{Spec}(A)$.

23. Sia A un anello, poniamo $X = \operatorname{Spec}(A)$ e sia U un aperto fondamentale di X (ossia, $U = X_f$ per qualche $f \in A$: Capitolo 1, Esercizio 17).

i) Se $U = X_f$, provare che l'anello $A(U) = A_f$ dipende soltanto da U e non da f.

ii) Sia $U' = X_g$ un altro aperto fondamentale tale che $U' \subseteq U$. Dimostrare che esiste un'equazione della forma $g^n = uf$ per qualche intero $n > 0$ e qualche $u \in A$, e utilizzare ciò per definire un omomorfismo $\rho\colon A(U) \to A(U')$ (ossia, $A_f \to A_g$)

mandando a/f^m in au^m/g^{mn}. Provare che ρ dipende soltanto da U e U'. Tale omomorfismo prende il nome di *omomorfismo di restrizione*.

iii) Se $U = U'$, allora ρ è l'applicazione identica.

iv) Se $U \supseteq U' \supseteq U''$ sono aperti fondamentali di X, dimostrare che il diagramma

$$\begin{tikzcd} A(U) \arrow[rr] \arrow[dr] & & A(U'') \\ & A(U') \arrow[ur] & \end{tikzcd}$$

(in cui le frecce sono omomorfismi di restrizione) è commutativo.

v) Sia $x\,(= \mathfrak{p})$ un punto di X. Provare che

$$\varinjlim_{U \ni x} A(U) \cong A_{\mathfrak{p}}.$$

Associando l'anello $A(U)$ a ciascun aperto fondamentale U di X e definendo gli omomorfismi di restrizione ρ, soddisfacenti alle condizioni iii) e iv) di cui sopra, si ottiene un *prefascio di anelli* sulla base di aperti $(X_f)_{f \in A}$. La v) dice che la spiga di tale prefascio in $x \in X$ è l'anello locale corrispondente $A_{\mathfrak{p}}$.

24. Provare che il prefascio dell'Esercizio 23 possiede la seguente proprietà. Sia $(U_i)_{i \in I}$ un ricoprimento di X con aperti fondamentali. Per ogni $i \in I$ sia s_i un elemento di $A(U_i)$ tale che, per ogni coppia di indici i, j, le immagini di s_i e s_j in $A(U_i \cap U_j)$ sono uguali. Allora esiste un unico elemento $s \in A\ (= A(X))$ la cui immagine in $A(U_i)$ è s_i, per ogni $i \in I$. (Ciò implica sostanzialmente che il prefascio è un *fascio*.)

25. Siano $f\colon A \to B$, $g\colon A \to C$ omomorfismi di anelli e sia $h\colon A \to B \otimes_A C$ definito ponendo $h(x) = f(x) \otimes 1\ (= 1 \otimes g(x))$. Siano X, Y, Z, T gli spettri primi di $A, B, C, B \otimes_A C$ rispettivamente. Allora $h^*(T) = f^*(Y) \cap g^*(Z)$.
[Sia $\mathfrak{p}$ un elemento di X, e sia $k = k(\mathfrak{p})$ il campo residuo in $\mathfrak{p}$. In virtù dell'Esercizio 21, la fibra $h^{*-1}(\mathfrak{p})$ è lo spettro di $(B \otimes_A C) \otimes_A k \cong (B \otimes_A k) \otimes_k (C \otimes_A k)$. Dunque $\mathfrak{p} \in h^*(T) \Leftrightarrow (B \otimes_A k) \otimes_k (C \otimes_A k) \neq 0 \Leftrightarrow B \otimes_A k \neq 0$ e $C \otimes_A k \neq 0 \Leftrightarrow \mathfrak{p} \in f^*(Y) \cap g^*(Z)$.]

26. Sia $(B_\alpha, g_{\alpha\beta})$ un sistema diretto di anelli e B il limite diretto. Per ogni α, sia $f_\alpha\colon A \to B_\alpha$ un omomorfismo di anelli tale che $g_{\alpha\beta} \circ f_\alpha = f_\beta$ ogni volta che $\alpha \leqslant \beta$ (ossia, i B_α formano un sistema diretto di A-algebre). Gli omomorfismi f_α inducono un omomorfismo $f\colon A \to B$. Dimostrare che

$$f^*(\mathrm{Spec}(B)) = \bigcap_\alpha f_\alpha^*(\mathrm{Spec}(B_\alpha)).$$

[Sia $\mathfrak{p}$ un elemento di $\mathrm{Spec}(A)$. Allora $f^{*-1}(\mathfrak{p})$ è lo spettro di

$$B \otimes_A k(\mathfrak{p}) \cong \varinjlim (B_\alpha \otimes_A k(\mathfrak{p}))$$

(poiché i prodotti tensoriali commutano con i limiti diretti: Capitolo 2, Esercizio 20). In virtú dell'Esercizio 21 del Capitolo 2 si ha che $f^{*-1}(\mathfrak{p}) = \emptyset$ se, e soltanto se, $B_\alpha \otimes_A k(\mathfrak{p}) = 0$ per qualche α, ossia, se, e soltanto se, $f_\alpha^{*-1}(\mathfrak{p}) = \emptyset$.]

27. i) Sia $f_\alpha\colon A \to B_\alpha$ una famiglia arbitraria di A-algebre e sia $f\colon A \to B$ il loro prodotto tensoriale sopra A (Capitolo 2, Esercizio 23). Allora

$$f^*(\mathrm{Spec}(B)) = \bigcap_\alpha f_\alpha^*(\mathrm{Spec}(B_\alpha)).$$

[Utilizzare gli Esercizi 25 e 26.]

ii) Sia $f_\alpha\colon A \to B_\alpha$ una qualsiasi famiglia finita di A-algebre e sia $B = \prod_\alpha B_\alpha$. Definiamo $f\colon A \to B$ ponendo $f(x) = (f_\alpha(x))$. Allora $f^*(\mathrm{Spec}(B)) = \bigcup_\alpha f_\alpha^*(\mathrm{Spec}(B_\alpha))$.

iii) Dunque i sottoinsiemi di $X = \mathrm{Spec}(A)$ della forma $f^*(\mathrm{Spec}(B))$, dove $f\colon A \to B$ è un omomorfismo di anelli, soddisfano gli assiomi per i chiusi di uno spazio topologico. La topologia associata è la topologia *costruibile* su X. Essa è piú fine della topologia di Zariski (ossia, vi sono piú aperti o, in modo equivalente, piú chiusi).

iv) Denotiamo con X_C l'insieme X dotato della topologia costruibile. Provare che X_C è quasi-compatto.

28. (Continuazione dell'Esercizio 27.)

i) Per ogni elemento $g \in A$, l'insieme X_g (Capitolo 1, Esercizio 17) è simultaneamente aperto e chiuso nella topologia costruibile.

ii) Denotiamo con C' la topologia meno fine su X per la quale gli insiemi X_g sono simultaneamente aperti e chiusi, e con $X_{C'}$ l'insieme X dotato di tale topologia. Dimostrare che $X_{C'}$ è uno spazio di Hausdorff.

iii) Dedurre che l'applicazione identica $X_C \to X_{C'}$ è un omeomorfismo. Ne segue che un sottoinsieme E di X è della forma $f^*(\mathrm{Spec}(B))$ per qualche $f: A \to B$ se, e soltanto se, è chiuso nella topologia C'.

iv) Lo spazio topologico X_C è compatto, di Hausdorff e totalmente sconnesso.

29. Sia $f: A \to B$ un omomorfismo di anelli. Dimostrare che f^*: $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ è un'applicazione continua e *chiusa* (ossia, manda sottoinsiemi chiusi in sottoinsiemi chiusi) rispetto alla topologia costruibile.

30. Provare che la topologia di Zariski e la topologia costruibile su $\mathrm{Spec}(A)$ coincidono se, e soltanto se, $A/\mathfrak{N}$ è assolutamente piatto (dove $\mathfrak{N}$ è il nilradicale di A). [Utilizzare l'Esercizio 11.]

Capitolo quarto

Decomposizione primaria

La decomposizione di un ideale in ideali primari è, per tradizione, un argomento fondamentale della teoria degli ideali. Essa fornisce le basi algebriche per decomporre una varietà algebrica nelle sue componenti irriducibili, anche se conviene sottolineare che la situazione algebrica è piú complicata di quello che la geometria intuitiva lascerebbe supporre. Da un altro punto di vista, la decomposizione primaria fornisce una generalizzazione della fattorizzazione di un numero intero come prodotto di potenze di numeri primi. Nella trattazione moderna, in cui si insiste molto sulla localizzazione, la decomposizione primaria non è piú uno strumento centrale della teoria. Tuttavia, essa è ancora interessante di per sé e in questo capitolo stabiliremo i classici teoremi di unicità.

I prototipi di anelli commutativi sono $\mathbf{Z}$ e l'anello dei polinomi $k[x_1, \ldots, x_n]$ dove k è un campo; entrambi sono domini a fattorizzazione unica. Ciò non è vero per anelli commutativi arbitrari, anche nel caso di domini di integrità (l'esempio classico è l'anello $\mathbf{Z}[\sqrt{-5}]$, in cui l'elemento 6 possiede due fattorizzazioni sostanzialmente distinte, $2 \quad 3$ e $(1 + \sqrt{-5})(1 - \sqrt{-5})$). Tuttavia, vale una forma generalizzata di "fattorizzazione unica" per gli *ideali* (non per gli elementi) in una vasta classe di anelli (gli anelli noetheriani).

Un ideale primo in un anello A è in un certo senso una generalizzazione di un numero primo. La generalizzazione corrispondente per la potenza di un numero primo è un ideale primario. Un ideale $\mathfrak{q}$ in un anello A è *primario*, se $\mathfrak{q} \neq A$ e se

$$xy \in \mathfrak{q} \Rightarrow x \in \mathfrak{q} \text{ oppure } y^n \in \mathfrak{q} \text{ per qualche intero } n > 0.$$

In altre parole,

$$\mathfrak{q} \text{ è primario} \Leftrightarrow A/\mathfrak{q} \neq 0 \text{ e ogni divisore dello zero in } A/\mathfrak{q} \text{ è nilpotente.}$$

Chiaramente ogni ideale primo è primario. Inoltre la contrazione di un ideale primario è primario, poiché se $f: A \to B$ è un omomorfismo di anelli e $\mathfrak{q}$ è un ideale primario in B, allora $A/\mathfrak{q}^c$ è isomorfo ad un subanello di $B/\mathfrak{q}$.

Proposizione 4.1. *Sia $\mathfrak{q}$ un ideale primario in un anello A. Allora $r(\mathfrak{q})$ è il più piccolo ideale primo che contiene $\mathfrak{q}$.*

Dimostrazione. In virtú di (1.14), basta far vedere che $\mathfrak{p} = r(\mathfrak{q})$ è primo. Se $xy \in r(\mathfrak{q})$, allora $(xy)^m \in \mathfrak{q}$ per qualche $m > 0$, e pertanto $x^m \in \mathfrak{q}$ oppure $y^{mn} \in \mathfrak{q}$ per qualche $n > 0$; ossia, $x \in r(\mathfrak{q})$ oppure $y \in r(\mathfrak{q})$. ■

Se $\mathfrak{p} = r(\mathfrak{q})$, allora $\mathfrak{q}$ si dice $\mathfrak{p}$-*primario*.

Esempi. 1) Gli ideali primari in $\mathbf{Z}$ sono (0) e (p^n), dove p è un numero primo. Infatti questi sono gli unici ideali di $\mathbf{Z}$ con radicale primo, e si verifica immediatamente che essi sono primari.

2) Sia $A = k[x, y]$, $\mathfrak{q} = (x, y^2)$. Allora $A/\mathfrak{q} \cong k[y]/(y^2)$, in cui i divisori dello zero sono tutti i multipli di y, quindi sono nilpotenti. Ne segue che $\mathfrak{q}$ è primario, e il suo radicale $\mathfrak{p}$ è (x, y). Si ha $\mathfrak{p}^2 \subset \mathfrak{q} \subset \mathfrak{p}$ (inclusioni strette), sicché un ideale primario non è necessariamente una potenza di un ideale primo.

3) Viceversa, una potenza di un ideale primo $\mathfrak{p}^n$ non è necessariamente un ideale primario, anche se il suo radicale è l'ideale primo $\mathfrak{p}$. Per esempio, sia $A = k[x, y, z]/(xy - z^2)$ e denotiamo con $\bar{x}, \bar{y}, \bar{z}$, rispettivamente, le immagini di x, y, z in A. Allora $\mathfrak{p} = (\bar{x}, \bar{z})$ è primo (poiché $A/\mathfrak{p} \cong k[y]$, il quale è un dominio di integrità); si ha $\bar{x}\bar{y} = \bar{z}^2 \in \mathfrak{p}^2$, ma $\bar{x} \notin \mathfrak{p}^2$ e $\bar{y} \notin r(\mathfrak{p}^2) = \mathfrak{p}$; dunque $\mathfrak{p}^2$ non è primario. Tuttavia, vale il seguente risultato:

Proposizione 4.2. *Se $r(\mathfrak{a})$ è massimale, allora $\mathfrak{a}$ è primario. In particolare, le potenze di un ideale massimale $\mathfrak{m}$ sono $\mathfrak{m}$-primarie.*

Dimostrazione. Sia $r(\mathfrak{a}) = \mathfrak{m}$. L'immagine di $\mathfrak{m}$ in $A/\mathfrak{a}$ è il nilradicale di $A/\mathfrak{a}$, dunque $A/\mathfrak{a}$ possiede un unico ideale primo, in virtú di (1.8). Pertanto ogni elemento di $A/\mathfrak{a}$ o è invertibile oppure è nilpotente, e quindi ogni divisore dello zero in $A/\mathfrak{a}$ è nilpotente. ■

Passiamo ora a studiare le espressioni di un ideale come *intersezione di ideali primari*. Dimostriamo innanzitutto due lemmi:

Lemma 4.3. *Se* $\mathfrak{q}_i$ $(1 \leqslant i \leqslant n)$ *sono* $\mathfrak{p}$*-primari, allora* $\mathfrak{q} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *è* $\mathfrak{p}$*-primario.*

Dimostrazione. $r(\mathfrak{q}) = r(\bigcap_{i=1}^{n} \mathfrak{q}_i) = \bigcap r(\mathfrak{q}_i) = \mathfrak{p}$. Sia $xy \in \mathfrak{q}, y \notin \mathfrak{q}$. Allora, per qualche indice i si ha $xy \in \mathfrak{q}_i$ e $y \notin \mathfrak{q}_i$, da cui $x \in \mathfrak{p}$, giacché $\mathfrak{q}_i$ è $\mathfrak{p}$-primario. ∎

Lemma 4.4. *Sia* $\mathfrak{q}$ *un ideale* $\mathfrak{p}$*-primario,* x *un elemento di* A*. Si ha:*

i) *se* $x \in \mathfrak{q}$*, allora* $(\mathfrak{q}:x) = (1)$;
ii) *se* $x \notin \mathfrak{q}$*, allora* $(\mathfrak{q}:x)$ *è* $\mathfrak{p}$*-primario, e pertanto* $r(\mathfrak{q}:x) = \mathfrak{p}$;
iii) *se* $x \notin \mathfrak{p}$*, allora* $(\mathfrak{q}:x) = \mathfrak{q}$.

Dimostrazione. i) e iii) seguono immediatamente dalle definizioni.
ii): se $y \in (\mathfrak{q}:x)$, allora $xy \in \mathfrak{q}$, da cui (poiché $x \notin \mathfrak{q}$) si ha $y \in \mathfrak{p}$. Dunque $\mathfrak{q} \subseteq (\mathfrak{q}:x) \subseteq \mathfrak{p}$; passando ai radicali, si ottiene $r(\mathfrak{q}:x) = \mathfrak{p}$. Sia $yz \in (\mathfrak{q}:x)$ con $y \notin \mathfrak{p}$; allora $xyz \in \mathfrak{q}$, da cui $xz \in \mathfrak{q}$, e quindi $z \in (\mathfrak{q}:x)$. ∎

Una *decomposizione primaria* di un ideale $\mathfrak{a}$ in A è un'espressione di $\mathfrak{a}$ come un'intersezione finita di ideali primari, diciamo

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i. \tag{1}$$

(In generale, una siffatta decomposizione primaria può non esistere; in questo capitolo, ci limiteremo a considerare gli ideali che possiedono una decomposizione primaria.) Se inoltre (i) i radicali $r(\mathfrak{q}_i)$ sono tutti distinti, e (ii) si ha $\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j$ $(1 \leqslant i \leqslant n)$, allora la decomposizione primaria (1) si dice *minimale* (o irridondante, o ridotta, o normale, ...). In virtú di (4.3) si può ottenere (i), e inoltre si possono omettere eventuali termini superflui in modo da ottenere (ii); dunque una qualsiasi decomposizione primaria può essere ricondotta ad una decomposizione minimale. Diremo che $\mathfrak{a}$ è *decomponibile* se possiede una decomposizione primaria.

Teorema 4.5. (I teorema di unicità). *Sia* $\mathfrak{a}$ *un ideale decomponibile e sia* $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *una decomposizione primaria minimale di* $\mathfrak{a}$*. Poniamo* $\mathfrak{p}_i = r(\mathfrak{q}_i)$ $(1 \leqslant i \leqslant n)$*. Allora gli ideali* $\mathfrak{p}_i$ *sono esattamente gli ideali primi che compaiono nell'insieme degli ideali* $r(\mathfrak{a}:x)$ $(x \in A)$*, e pertanto non dipendono dalla particolare decomposizione di* $\mathfrak{a}$.

Dimostrazione. Per un arbitrario elemento $x \in A$ si ha $(\mathfrak{a}:x) = (\bigcap \mathfrak{q}_i:x) = \bigcap (\mathfrak{q}_i:x)$, da cui $r(\mathfrak{a}:x) = \bigcap_{i=1}^{n} r(\mathfrak{q}_i:x) = \bigcap_{\mathfrak{q}_j \not\ni x} \mathfrak{p}_j$, stante (4.4). Supponiamo che $r(\mathfrak{a}:x)$ sia primo; allora, in virtú di (1.11), si ha $r(\mathfrak{a}:x) = \mathfrak{p}_j$ per qualche indice j. Dunque ogni ideale primo della forma $r(\mathfrak{a}:x)$ è uno degli ideali $\mathfrak{p}_j$. Viceversa, per ogni indice i esiste un elemento $x_i \notin \mathfrak{q}_i$, $x_i \in \bigcap_{j \neq i} \mathfrak{q}_j$, poiché la decomposizione è minimale; e si ha $r(\mathfrak{a}:x_i) = \mathfrak{p}_i$. ■

Osservazioni. 1) La dimostrazione sopra data, insieme con l'ultima parte di (4.4), prova che per ogni indice i esiste un elemento x_i di A tale che $(\mathfrak{a}:x_i)$ è $\mathfrak{p}_i$-primario.

2) Considerando $A/\mathfrak{a}$ come A-modulo, (4.5) equivale ad affermare che gli ideali $\mathfrak{p}_i$ sono precisamente gli ideali primi che compaiono come radicali di annullatori di elementi di $A/\mathfrak{a}$.

Esempio. Sia $\mathfrak{a} = (x^2, xy)$ in $A = k[x, y]$. Allora $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2^2$ dove $\mathfrak{p}_1 = (x)$, $\mathfrak{p}_2 = (x, y)$. L'ideale $\mathfrak{p}_2^2$ è primario in virtú di (4.2). Dunque gli ideali primi sono $\mathfrak{p}_1$, $\mathfrak{p}_2$. In questo esempio, $\mathfrak{p}_1 \subset \mathfrak{p}_2$; si ha $r(\mathfrak{a}) = \mathfrak{p}_1 \cap \mathfrak{p}_2 = \mathfrak{p}_1$, ma $\mathfrak{a}$ non è un ideale primario.

Gli ideali primi $\mathfrak{p}_i$ in (4.5) si dicono *appartenenti* ad $\mathfrak{a}$, oppure *associati* ad $\mathfrak{a}$. L'ideale $\mathfrak{a}$ è primario se, e soltanto se, possiede un unico ideale primo associato. Gli elementi minimali dell'insieme $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ sono chiamati gli ideali primi *minimali* o *isolati* appartenenti ad $\mathfrak{a}$. Gli altri prendono il nome di ideali primi *immersi*. Nell'esempio di cui sopra, $\mathfrak{p}_2 = (x, y)$ è immerso.

Proposizione 4.6. *Sia $\mathfrak{a}$ un ideale decomponibile. Allora ogni ideale primo $\mathfrak{p} \supseteq \mathfrak{a}$ contiene un ideale primo minimale appartenente ad $\mathfrak{a}$, sicché gli ideali primi minimali di $\mathfrak{a}$ sono precisamente gli elementi minimali nell'insieme di tutti gli ideali primi che contengono $\mathfrak{a}$.*

Dimostrazione. Se $\mathfrak{p} \supseteq \mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$, allora $\mathfrak{p} = r(\mathfrak{p}) \supseteq \bigcap r(\mathfrak{q}_i) = \bigcap \mathfrak{p}_i$. Ne segue, in virtú di (1.11), che $\mathfrak{p} \supseteq \mathfrak{p}_i$ per qualche i, e quindi $\mathfrak{p}$ contiene un ideale primo minimale di $\mathfrak{a}$. ■

Osservazioni. 1) I termini *isolato* e *immerso* provengono dalla geometria. Infatti, se $A = k[x_1, \ldots, x_n]$, dove k è un campo algebricamente chiuso, l'ideale $\mathfrak{a}$ individua una varietà $X \subseteq k^n$ (cfr. Capitolo 1, Esercizio 27). I primi minimali $\mathfrak{p}_i$ corrispondono alle componenti irriducibili di X, e i primi immersi corrispondono alle sottovarietà di queste, ossia, alle varietà *immerse* nelle componenti irriducibili. Così nell'esempio che precede (4.6), la varietà definita da $\mathfrak{a}$ è la retta $x = 0$, e l'ideale immerso $\mathfrak{p}_2 = (x, y)$ corrisponde all'origine $(0, 0)$.

2) *Non* è vero che tutte le componenti primarie sono indipendenti dalla decomposizione. Per esempio $(x^2, xy) = (x) \cap (x, y)^2 = (x) \cap \cap (x^2, y)$ sono due decomposizioni primarie minimali distinte. Tuttavia, sussistono alcune proprietà di unicità: cfr. (4.10).

Proposizione 4.7. *Sia* $\mathfrak{a}$ *un ideale decomponibile,* $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ *una decomposizione primaria minimale, e sia* $\mathfrak{p}_i = r(\mathfrak{q}_i)$. *Allora*

$$\bigcup_{i=1}^{n} \mathfrak{p}_i = \{x \in A : (\mathfrak{a} : x) \neq \mathfrak{a}\}.$$

In particolare, se l'ideale zero è decomponibile, l'insieme D dei divisori dello zero di A è l'unione degli ideali primi appartenenti a 0.

Dimostrazione. Se $\mathfrak{a}$ è decomponibile, allora 0 è decomponibile in $A/\mathfrak{a}$: precisamente $0 = \bigcap \bar{\mathfrak{q}}_i$, dove $\bar{\mathfrak{q}}_i$ è l'immagine di $\mathfrak{q}_i$ in $A/\mathfrak{a}$ ed è primario. Dunque è sufficiente provare l'ultima parte di (4.7). In virtú di (1.15) si ha $D = \bigcup_{x \neq 0} r(0 : x)$; dalla dimostrazione di (4.5) si ha $r(0:x) = \bigcap_{\mathfrak{q}_j \not\ni x} \mathfrak{p}_j \subseteq \mathfrak{p}_j$ per qualche j, da cui $D \subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$. Ma, ancora in virtú di (4.5), ciascun $\mathfrak{p}_i$ è della forma $r(0:x)$ per qualche elemento $x \in A$, e quindi $\bigcup \mathfrak{p}_i \subseteq D$. ∎

Dunque (se l'ideale zero è decomponibile)

$$\begin{aligned} D &= \text{insieme dei divisori dello zero} \\ &= \bigcup \text{ di tutti gli ideali primi appartenenti a } 0; \\ \mathfrak{N} &= \text{insieme degli elementi nilpotenti} \\ &= \bigcap \text{ di tutti i primi minimali appartenenti a } 0. \end{aligned}$$

Passiamo ora ad esaminare il comportamento degli ideali primari rispetto alla localizzazione.

Proposizione 4.8. *Sia S una parte moltiplicativa di A, e sia $\mathfrak{q}$ un ideale $\mathfrak{p}$-primario.*

i) *Se* $S \cap \mathfrak{p} \neq \emptyset$, *allora* $S^{-1}\mathfrak{q} = S^{-1}A$.

ii) *Se $S \cap \mathfrak{p} = \emptyset$, allora $S^{-1}\mathfrak{q}$ è $S^{-1}\mathfrak{p}$-primario e la sua contrazione in A è $\mathfrak{q}$.*

Dunque ideali primari corrispondono ad ideali primari nella corrispondenza (3.11) *tra gli ideali di $S^{-1}A$ e gli ideali contratti in A.*

Dimostrazione. i) Se $s \in S \cap \mathfrak{p}$, allora $s^n \in S \cap \mathfrak{q}$ per qualche $n > 0$; dunque $S^{-1}\mathfrak{q}$ contiene $s^n/1$, che è un elemento invertibile in $S^{-1}A$.

ii) Se $S \cap \mathfrak{p} = \emptyset$, allora $s \in S$ e $as \in \mathfrak{q}$ implicano $a \in \mathfrak{q}$, da cui $\mathfrak{q}^{ec} = \mathfrak{q}$, stante (3.11). Inoltre, ancora in virtú di (3.11), si ha $r(\mathfrak{q}^e) = r(S^{-1}\mathfrak{q}) = S^{-1}r(\mathfrak{q}) = S^{-1}\mathfrak{p}$. Si verifica direttamente che $S^{-1}\mathfrak{q}$ è primario. Infine, la contrazione di un ideale primario è un ideale primario. ∎

Per un qualsiasi ideale $\mathfrak{a}$ ed un'arbitraria parte moltiplicativa S in A, la contrazione in A dell'ideale $S^{-1}\mathfrak{a}$ viene denotata con $S(\mathfrak{a})$.

Proposizione 4.9. *Sia S una parte moltiplicativa di A e sia $\mathfrak{a}$ un ideale decomponibile. Sia $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ una decomposizione primaria minimale di $\mathfrak{a}$. Poniamo $\mathfrak{p}_i = r(\mathfrak{q}_i)$ e supponiamo che gli ideali $\mathfrak{q}_i$ siano numerati in modo tale che S incontra $\mathfrak{p}_{m+1}, \ldots, \mathfrak{p}_n$* ma non $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Allora

$$S^{-1}\mathfrak{a} = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i, \qquad S(\mathfrak{a}) = \bigcap_{i=1}^{m} \mathfrak{q}_i,$$

e si tratta, in entrambi i casi, di decomposizioni primarie minimali.

Dimostrazione. $S^{-1}\mathfrak{a} = \bigcap_{i=1}^{n} S^{-1}\mathfrak{q}_i$ (cfr. (3.11)) $= \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i$ (cfr. (4.8)), e $S^{-1}\mathfrak{q}_i$ è $S^{-1}\mathfrak{p}_i$-primario per $i = 1, \ldots, m$. Poiché gli ideali $\mathfrak{p}_i$ sono distinti, tali risultano gli ideali $S^{-1}\mathfrak{p}_i$ $(1 \leqslant i \leqslant m)$, sicché si ottiene una decomposizione primaria minimale. Contraendo ambo i membri, si ha

$$S(\mathfrak{a}) = (S^{-1}\mathfrak{a})^c = \bigcap_{i=1}^{m} (S^{-1}\mathfrak{q}_i)^c = \bigcap_{i=1}^{m} \mathfrak{q}_i,$$

ancora in virtú di (4.8). ∎

Un insieme Σ di ideali primi appartenenti ad $\mathfrak{a}$ si dice *isolato* se soddisfa la seguente condizione: se $\mathfrak{p}'$ è un ideale primo appartenente ad $\mathfrak{a}$ e $\mathfrak{p}' \subseteq \mathfrak{p}$ per qualche $\mathfrak{p} \in \Sigma$, allora $\mathfrak{p}' \in \Sigma$.

Sia Σ un insieme isolato di ideali primi appartenenti ad $\mathfrak{a}$, e sia $S = A - \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}$. Allora S è una parte moltiplicativa e, per un qualsiasi ideale primo $\mathfrak{p}'$ appartenente ad $\mathfrak{a}$, si ha

$$\mathfrak{p}' \in \Sigma \Rightarrow \mathfrak{p}' \cap S = \emptyset;$$
$$\mathfrak{p}' \notin \Sigma \Rightarrow \mathfrak{p}' \not\subseteq \bigcup_{\mathfrak{p}\in\Sigma} \mathfrak{p}\ (\text{cfr. } (1.11)) \Rightarrow \mathfrak{p}' \cap S \neq \emptyset.$$

Dunque, da (4.9) si deduce:

Teorema 4.10. (II teorema di unicità). *Sia $\mathfrak{a}$ un ideale decomponibile, sia $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ una decomposizione primaria minimale di $\mathfrak{a}$, e sia $\{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}\}$ un insieme isolato di ideali primi di $\mathfrak{a}$. Allora l'ideale $\mathfrak{q}_{i_1} \cap \ldots \cap \mathfrak{q}_{i_m}$ è indipendente dalla decomposizione.*

In particolare:

Corollario 4.11. *Le componenti primarie isolate (ossia, le componenti primarie $\mathfrak{q}_i$ corrispondenti agli ideali primi minimali $\mathfrak{p}_i$) sono univocamente determinate da $\mathfrak{a}$.*

Dimostrazione di (4.10). Si ha $\mathfrak{q}_{i_1} \cap \ldots \cap \mathfrak{q}_{i_m} = S(\mathfrak{a})$ dove $S = A - \mathfrak{p}_{i_1} \cup \ldots \cup \mathfrak{p}_{i_m}$, dunque tale intersezione dipende soltanto da $\mathfrak{a}$ (poiché gli ideali $\mathfrak{p}_i$ dipendono soltanto da $\mathfrak{a}$). ■

Osservazione. D'altra parte, le componenti primarie immerse non sono univocamente determinate da $\mathfrak{a}$, in generale. Se A è un anello noetheriano, ciascuna componente immersa può essere scelta infatti in infiniti modi (cfr. Capitolo 8, Esercizio 1).

Esercizi

1. Se un ideale $\mathfrak{a}$ possiede una decomposizione primaria, allora $\mathrm{Spec}(A/\mathfrak{a})$ possiede soltanto un numero finito di componenti irriducibili.
2. Se $\mathfrak{a} = r(\mathfrak{a})$, allora $\mathfrak{a}$ non possiede ideali primi immersi.
3. Se A è assolutamente piatto, ogni ideale primario è massimale.
4. Nell'anello dei polinomi $\mathbf{Z}[t]$, l'ideale $\mathfrak{m} = (2, t)$ è massimale e l'ideale $\mathfrak{q} = (4, t)$ è $\mathfrak{m}$-primario, ma non è una potenza di $\mathfrak{m}$.

5. Nell'anello dei polinomi $K[x, y, z]$ dove K è un campo e x, y, z sono indeterminate indipendenti, sia $\mathfrak{p}_1 = (x, y)$, $\mathfrak{p}_2 = (x, z)$, $\mathfrak{m} = (x, y, z)$; $\mathfrak{p}_1$ e $\mathfrak{p}_2$ sono ideali primi, e $\mathfrak{m}$ è massimale. Sia $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$. Provare che $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ è una decomposizione primaria ridotta di $\mathfrak{a}$. Quali componenti sono isolate e quali sono immerse?

6. Sia X uno spazio compatto di Hausdorff infinito, $C(X)$ l'anello delle funzioni continue a valori reali su X (Capitolo 1, Esercizio 26). L'ideale nullo è decomponibile in tale anello?

7. Sia A un anello e sia $A[x]$ l'anello dei polinomi in una indeterminata sopra A. Per ogni ideale $\mathfrak{a}$ di A, denotiamo con $\mathfrak{a}[x]$ l'insieme di tutti i polinomi in $A[x]$ a coefficienti in $\mathfrak{a}$.

   i) $\mathfrak{a}[x]$ è l'estensione di $\mathfrak{a}$ ad $A[x]$.
   ii) Se $\mathfrak{q}$ è un ideale $\mathfrak{p}$-primario in A, allora $\mathfrak{q}[x]$ è un ideale $\mathfrak{p}[x]$-primario in $A[x]$. [Utilizzare l'Esercizio 2 del Capitolo 1.]
   iii) Se $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$ è una decomposizione primaria minimale in A, allora $\mathfrak{a}[x] = \bigcap_{i=1}^{n} \mathfrak{q}_i[x]$ è una decomposizione primaria minimale in $A[x]$.
   iv) Se $\mathfrak{p}$ è un ideale primo minimale di $\mathfrak{a}$, allora $\mathfrak{p}[x]$ è un ideale primo minimale di $\mathfrak{a}[x]$.

8. Sia k un campo. Dimostrare che nell'anello dei polinomi $k[x_1, \ldots, x_n]$ gli ideali $\mathfrak{p}_i = (x_1, \ldots, x_i)$ $(1 \leqslant i \leqslant n)$ sono primi e tutte le loro potenze sono ideali primari. [Utilizzare l'Esercizio 7.]

9. In un anello A, denotiamo con $D(A)$ l'insieme degli ideali primi $\mathfrak{p}$ che soddisfano alla seguente condizione: esiste un elemento $a \in A$ tale che $\mathfrak{p}$ è minimale nell'insieme degli ideali primi contenenti $(0:a)$. Provare che $x \in A$ è un divisore dello zero $\Leftrightarrow x \in \mathfrak{p}$ per qualche $\mathfrak{p} \in D(A)$.

   Sia S una parte moltiplicativa di A, e identifichiamo $\operatorname{Spec}(S^{-1}A)$ con la sua immagine in $\operatorname{Spec}(A)$ (Capitolo 3, Esercizio 21). Dimostrare che

$$D(S^{-1}A) = D(A) \cap \operatorname{Spec}(S^{-1}A).$$

   Se l'ideale nullo possiede una decomposizione primaria, provare che $D(A)$ è l'insieme degli ideali primi associati a 0.

10. Per un qualsiasi ideale primo $\mathfrak{p}$ in un anello A, denotiamo con $S_{\mathfrak{p}}(0)$ il nucleo dell'omomorfismo $A \to A_{\mathfrak{p}}$. Dimostrare che:

i) $S_{\mathfrak{p}}(0) \subseteq \mathfrak{p}$.
ii) $r(S_{\mathfrak{p}}(0)) = \mathfrak{p} \Leftrightarrow \mathfrak{p}$ è un ideale primo minimale di A.
iii) Se $\mathfrak{p} \supseteq \mathfrak{p}'$, allora $S_{\mathfrak{p}}(0) \subseteq S_{\mathfrak{p}'}(0)$.
iv) $\bigcap_{\mathfrak{p} \in D(A)} S_{\mathfrak{p}}(0) = 0$, dove $D(A)$ è definito nell'Esercizio 9.

11. Se $\mathfrak{p}$ è un ideale primo minimale di un anello A, provare che $S_{\mathfrak{p}}(0)$ (Esercizio 10) è il piú piccolo ideale $\mathfrak{p}$-primario.

Sia $\mathfrak{a}$ l'intersezione degli ideali $S_{\mathfrak{p}}(0)$ al variare di $\mathfrak{p}$ tra gli ideali primi minimali di A. Dimostrare che $\mathfrak{a}$ è contenuto nel nilradicale di A.

Supponiamo che l'ideale nullo sia decomponibile. Provare che $\mathfrak{a} = 0$ se e soltanto se ogni ideale primo di 0 è isolato.

12. Sia A un anello, S una parte moltiplicativa di A. Per un qualsiasi ideale $\mathfrak{a}$, denotiamo con $S(\mathfrak{a})$ la contrazione di $S^{-1}\mathfrak{a}$ in A. L'ideale $S(\mathfrak{a})$ prende il nome di *saturazione* di $\mathfrak{a}$ rispetto a S. Dimostrare che:

i) $S(\mathfrak{a}) \cap S(\mathfrak{b}) = S(\mathfrak{a} \cap \mathfrak{b})$
ii) $S(r(\mathfrak{a})) = r(S(\mathfrak{a}))$
iii) $S(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a}$ incontra S
iv) $S_1(S_2(\mathfrak{a})) = (S_1S_2)(\mathfrak{a})$.

Se $\mathfrak{a}$ possiede una decomposizione primaria, provare che l'insieme degli ideali $S(\mathfrak{a})$ (al variare di S tra tutte le parti moltiplicative di A) è finito.

13. Sia A un anello e $\mathfrak{p}$ un ideale primo di A. Si definisce *potenza simbolica n-esima di* $\mathfrak{p}$ l'ideale (con la notazione dell'Esercizio 12)

$$\mathfrak{p}^{(n)} = S_{\mathfrak{p}}(\mathfrak{p}^n)$$

dove $S_{\mathfrak{p}} = A - \mathfrak{p}$. Dimostrare che:

i) $\mathfrak{p}^{(n)}$ è un ideale $\mathfrak{p}$-primario;
ii) se $\mathfrak{p}^n$ possiede una decomposizione primaria, allora $\mathfrak{p}^{(n)}$ è la sua componente $\mathfrak{p}$-primaria;
iii) se $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$ possiede una decomposizione primaria, allora $\mathfrak{p}^{(m+n)}$ è la sua componente $\mathfrak{p}$-primaria;
iv) $\mathfrak{p}^{(n)} = \mathfrak{p}^n \Leftrightarrow \mathfrak{p}^n$ è $\mathfrak{p}$-primario.

14. Sia $\mathfrak{a}$ un ideale decomponibile in un anello A e sia $\mathfrak{p}$ un elemento massimale dell'insieme degli ideali $(\mathfrak{a}:x)$, dove $x \in A$ e $x \notin \mathfrak{a}$. Dimostrare che $\mathfrak{p}$ è un ideale primo appartenente ad $\mathfrak{a}$.

15. Sia $\mathfrak{a}$ un ideale decomponibile in un anello A, sia Σ un insieme isolato di ideali primi appartenenti ad $\mathfrak{a}$, e sia $\mathfrak{q}_\Sigma$ l'intersezione delle componenti primarie corrispondenti. Sia f un elemento di A tale che, per ogni ideale primo $\mathfrak{p}$ appartenente ad $\mathfrak{a}$, si ha $f \in \mathfrak{p} \Leftrightarrow \mathfrak{p} \notin \Sigma$, e sia S_f l'insieme di tutte le potenze di f. Provare che $\mathfrak{q}_\Sigma = S_f(\mathfrak{a}) = (\mathfrak{a} : f^n)$ per ogni intero n abbastanza grande.

16. Se A è un anello in cui ogni ideale possiede una decomposizione primaria, dimostrare che ogni anello di frazioni $S^{-1}A$ gode della medesima proprietà.

17. Sia A un anello con la seguente proprietà:

    (L1) Per ogni ideale $\mathfrak{a} \neq (1)$ in A e per ogni ideale primo $\mathfrak{p}$, esiste un elemento $x \notin \mathfrak{p}$ tale che $S_\mathfrak{p}(\mathfrak{a}) = (\mathfrak{a} : x)$, dove $S_\mathfrak{p} = A - \mathfrak{p}$.

    Allora ogni ideale di A è un'intersezione (eventualmente infinita) di ideali primari.

    [Sia $\mathfrak{a}$ un ideale $\neq (1)$ in A, e sia $\mathfrak{p}_1$ un elemento minimale dell'insieme degli ideali primi contenenti $\mathfrak{a}$. Allora $\mathfrak{q}_1 = S_{\mathfrak{p}_1}(\mathfrak{a})$ è $\mathfrak{p}_1$-primario (in virtú dell'Esercizio 11), e $\mathfrak{q}_1 = (\mathfrak{a} : x)$ per qualche $x \notin \mathfrak{p}_1$. Dimostrare che $\mathfrak{a} = \mathfrak{q}_1 \cap (\mathfrak{a} + (x))$.

    Sia ora $\mathfrak{a}_1$ un elemento massimale dell'insieme degli ideali $\mathfrak{b} \supseteq \mathfrak{a}$ tali che $\mathfrak{q}_1 \cap \mathfrak{b} = \mathfrak{a}$, e scegliamo $\mathfrak{a}_1$ in modo tale che $x \in \mathfrak{a}_1$, e pertanto $\mathfrak{a}_1 \nsubseteq \mathfrak{p}_1$. Ripetiamo la costruzione partendo da $\mathfrak{a}_1$, e cosí via. Dopo n passi si ha $\mathfrak{a} = \mathfrak{q}_1 \cap \quad \cap \mathfrak{q}_n \cap \mathfrak{a}_n$, dove i $\mathfrak{q}_i$ sono ideali primari, $\mathfrak{a}_n$ è massimale tra gli ideali $\mathfrak{b}$ contenenti $\mathfrak{a}_{n-1} = \mathfrak{a}_n \cap \mathfrak{q}_n$ tali che $\mathfrak{a} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n \cap \mathfrak{b}$, e $\mathfrak{a}_n \nsubseteq \mathfrak{p}_n$. Se in qualche passo si ha $\mathfrak{a}_n = (1)$, il procedimento si arresta, e $\mathfrak{a}$ risulta un'intersezione finita di ideali primari. Altrimenti, si procede per induzione transfinita, osservando che ogni ideale $\mathfrak{a}_n$ contiene strettamente $\mathfrak{a}_{n-1}$.]

18. Consideriamo la seguente condizione su un anello A:

    (L2) Dati un ideale $\mathfrak{a}$ e una catena discendente $S_1 \supseteq S_2 \supseteq \quad \supseteq S_n \supseteq \ldots$ di parti moltiplicative di A, esiste un intero n tale che $S_n(\mathfrak{a}) = S_{n+1}(\mathfrak{a}) = \quad$ Dimostrare che le seguenti affermazioni sono equivalenti:

    i) Ogni ideale di A possiede una decomposizione primaria;
    ii) A soddisfa (L1) e (L2).

    [Per dimostrare che $i) \Rightarrow ii)$, utilizzare gli Esercizi 12 e 15. Per ottenere l'implicazione opposta provare, con le notazioni della dimostrazione dell'Esercizio 17, che se $S_n = S_{\mathfrak{p}_1} \cap \quad \cap S_{\mathfrak{p}_n}$ allora S_n incontra $\mathfrak{a}_n$, da cui $S_n(\mathfrak{a}_n) = (1)$, e pertanto $S_n(\mathfrak{a}) = \mathfrak{q}_1 \cap$

$\cap\, \mathfrak{q}_n$. Ora utilizzare (L2) per concludere che la costruzione ha termine necessariamente dopo un numero finito di passi.]

19. Sia A un anello e $\mathfrak{p}$ un ideale primo di A. Dimostrare che ogni ideale $\mathfrak{p}$-primario contiene $S_{\mathfrak{p}}(0)$, il nucleo dell'omomorfismo canonico $A \to A_{\mathfrak{p}}$.

    Supponiamo che A soddisfi alla seguente condizione: per ogni ideale primo $\mathfrak{p}$, l'intersezione di tutti gli ideali $\mathfrak{p}$-primari di A è uguale a $S_{\mathfrak{p}}(0)$. (Gli anelli noetheriani verificano tale condizione: cfr. il Capitolo 10.) Siano $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideali primi distinti, nessuno dei quali sia un ideale primo minimale di A. Allora esiste un ideale $\mathfrak{a}$ in A i cui ideali primi associati sono $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$.

    [Si procede per induzione su n. Il caso $n = 1$ è banale (basta prendere $\mathfrak{a} = \mathfrak{p}_1$). Supponiamo $n > 1$ e sia $\mathfrak{p}_n$ un elemento massimale dell'insieme $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. In virtú dell'ipotesi induttiva, esiste un ideale $\mathfrak{b}$ ed una decomposizione primaria minimale $\mathfrak{b} = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_{n-1}$, dove ciascun ideale $\mathfrak{q}_i$ è $\mathfrak{p}_i$-primario. Se $\mathfrak{b} \subseteq S_{\mathfrak{p}_n}(0)$, sia $\mathfrak{p}$ un ideale primo minimale di A contenuto in $\mathfrak{p}_n$. Allora $S_{\mathfrak{p}_n}(0) \subseteq S_{\mathfrak{p}}(0)$, da cui $\mathfrak{b} \subseteq S_{\mathfrak{p}}(0)$. Passando ai radicali e utilizzando l'Esercizio 10, si ha $\mathfrak{p}_1 \cap \quad \cap\, \mathfrak{p}_{n-1} \subseteq \mathfrak{p}$, sicché $\mathfrak{p}_i \subseteq \mathfrak{p}$ per qualche indice i, dunque $\mathfrak{p}_i = \mathfrak{p}$, essendo $\mathfrak{p}$ minimale. Ciò è una contraddizione poiché nessun ideale $\mathfrak{p}_i$ è minimale. Ne segue che $\mathfrak{b} \nsubseteq S_{\mathfrak{p}_n}(0)$ e pertanto esiste un ideale $\mathfrak{p}_n$-primario $\mathfrak{q}_n$ tale che $\mathfrak{b} \nsubseteq \mathfrak{q}_n$. Provare che $\mathfrak{a} = \mathfrak{q}_1 \cap \quad \cap\, \mathfrak{q}_n$ possiede le proprietà richieste.]

Decomposizione primaria dei moduli

Conviene sottolineare che tutti i risultati di questo capitolo possono essere rienunciati con riferimento ai moduli sopra un anello A. Gli esercizi seguenti indicano come ciò può esser fatto.

20. Sia M un A-modulo assegnato, N un sottomodulo di M. Si definisce il *radicale* di N in M nel modo seguente:

$$r_M(N) = \{x \in A : x^q M \subseteq N \text{ per qualche intero } q > 0\}.$$

    Provare che $r_M(N) = r(N:M) = r(\mathrm{Ann}\,(M/N))$. In particolare, $r_M(N)$ è un *ideale*.

    Enunciare e dimostrare le formule per r_M analoghe a quelle date in (1.13).

21. Un elemento $x \in A$ definisce un endomorfismo ϕ_x di M, precisamente $m \mapsto xm$. L'elemento x si dice *divisore dello zero* (risp. *nilpo-*

tente) *in* M, se ϕ_x non è iniettivo (risp. è nilpotente). Un sottomodulo Q di M è *primario in* M, se $Q \neq M$ e ogni divisore dello zero in M/Q è nilpotente.

Provare che se Q è primario in M, allora $(Q:M)$ è un ideale primario e quindi $r_M(Q)$ è un ideale primo $\mathfrak{p}$. Si dice allora che Q è $\mathfrak{p}$-*primario* (in M).

Dimostrare gli enunciati analoghi di (4.3) e (4.4).

22. Una *decomposizione primaria di* N *in* M è una rappresentazione di N come un'intersezione

$$N = Q_1 \cap \qquad \cap Q_n$$

di sottomoduli primari di M; essa è una *decomposizione primaria minimale*, se gli ideali $\mathfrak{p}_i = r_M(Q_i)$ sono tutti distinti e se nessuna delle componenti Q_i può essere omessa nell'intersezione, ossia, se $Q_i \not\supseteq \bigcap_{j \neq i} Q_j \; (1 \leqslant i \leqslant n)$.

Dimostrare l'analogo di (4.5), ossia che gli ideali primi $\mathfrak{p}_i$ dipendono soltanto da N (e M). Essi prendono il nome di *ideali primi appartenenti a* N *in* M. Provare che essi risultano anche gli ideali primi appartenenti a 0 in M/N.

23. Enunciare e dimostrare gli analoghi di (4.6), ..., (4.11). (Non è restrittivo prendere $N = 0$.)

Capitolo quinto

Dipendenza integrale e valutazioni

Nella geometria algebrica classica le curve venivano spesso studiate proiettandole su una retta e considerando una curva come un rivestimento (ramificato) della retta. Ciò è del tutto analogo alla relazione che intercorre tra un campo di numeri e il campo razionale — o piuttosto tra i loro anelli degli interi — e il carattere algebrico comune è la nozione di dipendenza integrale. In questo capitolo proviamo alcuni risultati relativi alla dipendenza integrale. In particolare dimostriamo i teoremi di Cohen-Seidenberg (i teoremi del "going-up" e del "going-down") riguardanti gli ideali primi in una estensione intera. Negli esercizi alla fine, discutiamo la situazione algebro-geometrica e in particolare il Lemma di normalizzazione.

Diamo inoltre una breve trattazione delle valutazioni.

Dipendenza integrale

Sia B un anello, A un subanello di B (sicché $1 \in A$). Un elemento x di B si dice *intero* su A, se x è radice di un polinomio *monico* a coefficienti in A, ossia se x soddisfa ad un'equazione della forma

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0 \tag{1}$$

dove gli a_i sono elementi di A. È chiaro che ogni elemento di A è intero su A.

Esempio 5.0. $A = \mathbf{Z}$, $B = \mathbf{Q}$. Se un numero razionale $x = r/s$ è intero su $\mathbf{Z}$, dove r, s non hanno fattori comuni, si ha dalla (1)

$$r^n + a_1 r^{n-1} s + \cdots + a_n s^n = 0$$

essendo gli a_i numeri interi. Dunque s divide r^n, sicché $s = \pm 1$ e quindi $x \in \mathbf{Z}$.

Proposizione 5.1. *Le seguenti condizioni sono equivalenti*:

i) $x \in B$ *è intero su* A;

ii) $A[x]$ *è un* A*-modulo finitamente generato*;

iii) $A[x]$ *è contenuto in un subanello* C *di* B *tale che* C *è un* A*-modulo finitamente generato*;

iv) *Esiste un* $A[x]$*-modulo fedele* M *che è finitamente generato come* A*-modulo.*

Dimostrazione. i) $\Rightarrow$ ii). Dalla (1) si ha

$$x^{n+r} = -(a_1 x^{n+r-1} + \qquad + a_n x^r)$$

per ogni intero $r \geqslant 0$; dunque, per induzione, tutte le potenze positive di x appartengono all'A-modulo generato da $1, x, \ldots, x^{n-1}$. Pertanto $A[x]$ è generato (come A-modulo) da $1, x, \ldots, x^{n-1}$.

ii) $\Rightarrow$ iii). Basta prendere $C = A[x]$.

iii) $\Rightarrow$ iv). Basta prendere $M = C$, il quale è un $A[x]$-modulo fedele (giacché $yC = 0 \Rightarrow y \quad 1 = 0$).

iv) $\Rightarrow$ i). Ciò segue da (2.4) prendendo $\phi =$ moltiplicazione per x, e $\mathfrak{a} = A$ (si ha $xM \subseteq M$, essendo M un $A[x]$-modulo); poiché M è fedele, si ha $x^n + a_1 x^{n-1} + \qquad + a_n = 0$, essendo gli a_i opportuni elementi di A. ■

Corollario 5.2. *Siano* $x_1, \ldots, x_n$ *elementi di* B *interi su* A. *Allora l'anello* $A[x_1, \ldots, x_n]$ *è un* A*-modulo finitamente generato.*

Dimostrazione. Si procede per induzione su n. Il caso $n = 1$ è trattato in (5.1). Supponiamo $n > 1$, e poniamo $A_r = A[x_1, \ldots, x_r]$; allora, per l'ipotesi induttiva, A_{n-1} è un A-modulo finitamente generato. D'altra parte, $A_n = A_{n-1}[x_n]$ è un A_{n-1}-modulo finitamente generato (in virtú del caso $n = 1$, giacché x_n è intero su A_{n-1}). Dunque, in virtú di (2.16), A_n è un A-modulo finitamente generato. ■

Corollario 5.3. *L'insieme* C *degli elementi di* B *che sono interi su* A *è un subanello di* B *che contiene* A.

Dimostrazione. Se $x, y \in C$, allora $A[x, y]$ è un A-modulo finitamente generato, in virtú di (5.2). Dunque $x \pm y$ e xy sono interi su A, stante la iii) di (5.1). ■

L'anello C definito in (5.3) prende il nome di *chiusura integrale* di A in B. Se $C = A$, allora A si dice *integralmente chiuso in* B. Se $C = B$, l'anello B si dice *intero sopra* A.

Osservazione. Sia $f\colon A \to B$ un omomorfismo di anelli, cosicché B è una A-algebra. Allora f si dice *intero*, e B si dice una A-algebra *intera*, se B è intero sul suo subanello $f(A)$. Con questa terminologia, i risultati precedenti mostrano che

"tipo finito" + "intero" = "finito".

Corollario 5.4. *Se $A \subseteq B \subseteq C$ sono anelli e se B è intero su A, e C è intero su B, allora C è intero su A (transitività della dipendenza integrale).*

Dimostrazione. Preso comunque un elemento $x \in C$, si ha un'equazione

$$x^n + b_1x^{n-1} + \quad + b_n = 0 \qquad (b_i \in B).$$

L'anello $B' = A[b_1, \ldots, b_n]$ è un A-modulo finitamente generato in virtú di (5.2), e $B'[x]$ è un B'-modulo finitamente generato (poiché x è intero su B'). Dunque $B'[x]$ è un A-modulo finitamente generato (cfr. (2.16)) e pertanto x è intero su A, stante la iii) di (5.1). ∎

Corollario 5.5. *Siano $A \subseteq B$ anelli e sia C la chiusura integrale di A in B. Allora C è integralmente chiuso in B.*

Dimostrazione. Sia $x \in B$ intero su C. In virtú di (5.4) x è intero su A, sicché $x \in C$. ∎

La proposizione seguente mostra che la dipendenza integrale si conserva nel passaggio ai quozienti e agli anelli di frazioni:

Proposizione 5.6. *Siano $A \subseteq B$ anelli, e B intero su A.*

i) *Se $\mathfrak{b}$ è un ideale di B e $\mathfrak{a} = \mathfrak{b}^c = A \cap \mathfrak{b}$, allora $B/\mathfrak{b}$ è intero su $A/\mathfrak{a}$.*

ii) *Se S è una parte moltiplicativa di A, allora $S^{-1}B$ è intero su $S^{-1}A$.*

Dimostrazione. i) Se $x \in B$ si ha, diciamo, $x^n + a_1x^{n-1} + \quad + a_n = 0$, con $a_i \in A$. Per ottenere la tesi, basta ridurre tale equazione mod. $\mathfrak{b}$.

ii) Sia x/s un elemento arbitrario di $S^{-1}B (x \in B, s \in S)$. Allora dall'equazione sopra scritta si ha

$$(x/s)^n + (a_1/s)(x/s)^{n-1} + \quad + a_n/s^n = 0$$

ciò che prova che x/s è intero su $S^{-1}A$. ∎

Il teorema del going-up

Proposizione 5.7. *Siano $A \subseteq B$ domini di integrità e sia B intero su A. Allora B è un campo se e soltanto se A è un campo.*

Dimostrazione. Supponiamo che A sia un campo, e consideriamo un elemento $y \in B, y \neq 0$. Sia

$$y^n + a_1 y^{n-1} + \quad + a_n = 0 \qquad (a_i \in A)$$

un'equazione di dipendenza integrale per y di grado minimo. Poiché B è un dominio di integrità si ha $a_n \neq 0$, da cui $y^{-1} = -a_n^{-1}(y^{n-1} + + a_1 y^{n-2} + \quad + a_{n-1}) \in B$. Dunque B è un campo.

Viceversa, supponiamo che B sia un campo, e consideriamo un elemento $x \in A, x \neq 0$. Allora $x^{-1} \in B$, dunque è intero su A, sicché si ha un'equazione

$$x^{-m} + a_1' x^{-m+1} + \quad + a_m' = 0 \qquad (a_i' \in A).$$

Ne segue che $x^{-1} = -(a_1' + a_2' x + \quad + a_m' x^{m-1}) \in A$, dunque A è un campo. ■

Corollario 5.8. *Siano $A \subseteq B$ anelli, e B intero su A; sia $\mathfrak{q}$ un ideale primo di B e poniamo $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap A$. Allora $\mathfrak{q}$ è massimale se e soltanto se $\mathfrak{p}$ è massimale.*

Dimostrazione. In virtú di (5.6), $B/\mathfrak{q}$ è intero su $A/\mathfrak{p}$, e tali anelli sono entrambi domini di integrità. A questo punto, basta utilizzare (5.7). ■

Corollario 5.9. *Siano $A \subseteq B$ anelli, e B intero su A; siano $\mathfrak{q}, \mathfrak{q}'$ ideali primi di B tali che $\mathfrak{q} \subseteq \mathfrak{q}'$ e $\mathfrak{q}^c = \mathfrak{q}'^c = \mathfrak{p}$, diciamo. Allora risulta: $\mathfrak{q} = \mathfrak{q}'$.*

Dimostrazione. In virtú di (5.6), $B_\mathfrak{p}$ è intero su $A_\mathfrak{p}$. Sia $\mathfrak{m}$ l'estensione di $\mathfrak{p}$ in $A_\mathfrak{p}$ e siano $\mathfrak{n}, \mathfrak{n}'$, rispettivamente, le estensioni di $\mathfrak{q}, \mathfrak{q}'$ in $B_\mathfrak{p}$. Allora $\mathfrak{m}$ è l'ideale massimale di $A_\mathfrak{p}$; inoltre $\mathfrak{n} \subseteq \mathfrak{n}'$, e $\mathfrak{n}^c = \mathfrak{n}'^c = = \mathfrak{m}$. Da (5.8) segue che $\mathfrak{n}, \mathfrak{n}'$ sono massimali, sicché $\mathfrak{n} = \mathfrak{n}'$ e quindi, stante (3.11) (iv), $\mathfrak{q} = \mathfrak{q}'$. ■

Teorema 5.10. *Siano $A \subseteq B$ anelli, con B intero su A, e sia $\mathfrak{p}$ un ideale primo di A. Allora esiste un ideale primo $\mathfrak{q}$ di B tale che $\mathfrak{q} \cap A = \mathfrak{p}$.*

Dimostrazione. In virtú di (5.6), $B_{\mathfrak{p}}$ è intero su $A_{\mathfrak{p}}$, e il diagramma

$$\begin{tikzcd} A \arrow[r] \arrow[d, "\alpha"'] & B \arrow[d, "\beta"] \\ A_{\mathfrak{p}} \arrow[r] & B_{\mathfrak{p}} \end{tikzcd}$$

(in cui le frecce orizzontali sono iniettive) è commutativo. Sia $\mathfrak{n}$ un ideale massimale di $B_{\mathfrak{p}}$; allora $\mathfrak{m} = \mathfrak{n} \cap A_{\mathfrak{p}}$ è massimale (cfr. (5.8)), sicché è l'unico ideale massimale dell'anello locale $A_{\mathfrak{p}}$. Se poniamo $\mathfrak{q} = \beta^{-1}(\mathfrak{n})$, allora $\mathfrak{q}$ è primo e si ha $\mathfrak{q} \cap A = \alpha^{-1}(\mathfrak{m}) = \mathfrak{p}$. ∎

Teorema 5.11. (Teorema del "going-up"). *Siano $A \subseteq B$ anelli, con B intero su A; siano $\mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$ una catena di ideali primi di A e $\mathfrak{q}_1 \subseteq \ldots \subseteq \mathfrak{q}_m$ $(1 \leqslant m < n)$ una catena di ideali primi di B tali che $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ $(1 \leqslant i \leqslant m)$. Allora la catena $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_m$ può essere estesa ad una catena $\mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$ tale che $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ per $1 \leqslant i \leqslant n$.*

Dimostrazione. Procedendo per induzione ci si riduce immediatamente al caso in cui $m = 1, n = 2$. Poniamo $\bar{A} = A/\mathfrak{p}_1$, $\bar{B} = B/\mathfrak{q}_1$; allora $\bar{A} \subseteq \bar{B}$, e $\bar{B}$ è intero su $\bar{A}$ (cfr. (5.6)). Ne segue, in virtú di (5.10), che esiste un ideale primo $\bar{\mathfrak{q}}_2$ di $\bar{B}$ tale che $\bar{\mathfrak{q}}_2 \cap \bar{A} = \bar{\mathfrak{p}}_2$, l'immagine di $\mathfrak{p}_2$ in $\bar{A}$. Sollevando $\bar{\mathfrak{q}}_2$ in B si ottiene un ideale primo $\mathfrak{q}_2$ con le proprietà richieste. ∎

Domini di integrità integralmente chiusi. Il teorema del going-down

La proposizione (5.6)(ii) può essere migliorata:

Proposizione 5.12. *Siano $A \subseteq B$ anelli, e sia C la chiusura integrale di A in B. Sia S una parte moltiplicativa di A. Allora $S^{-1}C$ è la chiusura integrale di $S^{-1}A$ in $S^{-1}B$.*

Dimostrazione. In virtú di (5.6), $S^{-1}C$ è intero su $S^{-1}A$. Viceversa, se un elemento $b/s \in S^{-1}B$ è intero su $S^{-1}A$, allora si ha un'equazione della forma

$$(b/s)^n + (a_1/s_1)(b/s)^{n-1} + \cdots + a_n/s_n = 0$$

dove $a_i \in A$, $s_i \in S$ $(1 \leqslant i \leqslant n)$. Poniamo $t = s_1 \cdots s_n$ e moltiplichiamo ambo i membri di tale equazione per $(st)^n$. Allora essa diventa un'equazione di dipendenza integrale per l'elemento bt su A. Dunque $bt \in C$ e pertanto $b/s = bt/st \in S^{-1}C$. ∎

Un dominio di integrità si dice *integralmente chiuso* (senza ulteriori specificazioni) se è integralmente chiuso nel suo campo delle frazioni. Per esempio, **Z** è integralmente chiuso (cfr. (5.0)). La medesima argomentazione prova che un arbitrario dominio a fattorizzazione unica è integralmente chiuso. In particolare, un anello di polinomi $k[x_1, \dots, x_n]$ sopra un campo è integralmente chiuso.

La chiusura integrale è una proprietà locale:

Proposizione 5.13. *Sia A un dominio di integrità. Allora le seguenti condizioni sono equivalenti:*

i) *A è integralmente chiuso;*

ii) *$A_\mathfrak{p}$ è integralmente chiuso, per ogni ideale primo $\mathfrak{p}$;*

iii) *$A_\mathfrak{m}$ è integralmente chiuso, per ogni ideale massimale $\mathfrak{m}$.*

Dimostrazione. Sia K il campo delle frazioni di A, sia C la chiusura integrale di A in K, e sia $f\colon A \to C$ l'applicazione identica di A in C. Allora A è integralmente chiuso $\Leftrightarrow f$ è suriettiva, e in virtú di (5.12) $A_\mathfrak{p}$ (risp. $A_\mathfrak{m}$) è integralmente chiuso $\Leftrightarrow f_\mathfrak{p}$ (risp. $f_\mathfrak{m}$) è suriettiva. A questo punto basta utilizzare (3.9). ■

Siano $A \subseteq B$ anelli e sia $\mathfrak{a}$ un ideale di A. Un elemento di B si dice *intero su* $\mathfrak{a}$, se soddisfa ad un'equazione di dipendenza integrale su A in cui tutti i coefficienti appartengono ad $\mathfrak{a}$. La *chiusura integrale* di $\mathfrak{a}$ in B è l'insieme di tutti gli elementi di B che sono interi su $\mathfrak{a}$.

Lemma 5.14. *Sia C la chiusura integrale di A in B e denotiamo con $\mathfrak{a}^e$ l'estensione di $\mathfrak{a}$ in C. Allora la chiusura integrale di $\mathfrak{a}$ in B è il radicale di $\mathfrak{a}^e$ (e pertanto è chiusa rispetto all'addizione e alla moltiplicazione).*

Dimostrazione. Se un elemento $x \in B$ è intero su $\mathfrak{a}$, si ha un'equazione della forma

$$x^n + a_1x^{n-1} + \quad + a_n = 0$$

con $a_1, \dots, a_n$ in $\mathfrak{a}$. Dunque $x \in C$ e $x^n \in \mathfrak{a}^e$, ossia $x \in r(\mathfrak{a}^e)$. Viceversa, se $x \in r(\mathfrak{a}^e)$, allora $x^n = \sum_{i=1}^{k} a_i x_i$ per qualche $n > 0$, dove gli a_i sono elementi di $\mathfrak{a}$ e gli x_i sono elementi di C. Poiché ciascun x_i è intero su A, segue da (5.2) che $M = A[x_1, \dots, x_k]$ è un A-modulo finitamente generato, e inoltre $x^n M \subseteq \mathfrak{a}M$. Allora in virtú di (2.4) (prendendo $\phi =$ moltiplicazione per x^n), si ha che x^n è intero su $\mathfrak{a}$, sicché x è intero su $\mathfrak{a}$. ■

Proposizione 5.15. *Siano $A \subseteq B$ domini di integrità, con A integralmente chiuso, e sia $x \in B$ intero su un ideale $\mathfrak{a}$ di A. Allora x è algebrico sul campo delle frazioni K di A, e se il suo polinomio minimo su K è $t^n + a_1 t^{n-1} + \dots + a_n$, allora $a_1, \dots, a_n$ appartengono a $r(\mathfrak{a})$.*

Dimostrazione. È chiaro che x è algebrico su K. Sia L un'estensione di K (L campo) contenente tutti i coniugati $x_1, \dots, x_n$ di x. Ogni elemento x_i soddisfa alla medesima equazione di dipendenza integrale relativa a x, sicché ciascun x_i è intero su $\mathfrak{a}$. I coefficienti del polinomio minimo di x su K sono polinomi negli x_i e dunque, in virtú di (5.14), sono interi su $\mathfrak{a}$. Poiché A è integralmente chiuso, essi devono appartenere a $r(\mathfrak{a})$, ancora in virtú di (5.14). ■

Teorema 5.16. (Teorema del "going-down"). *Siano $A \subseteq B$ domini di integrità, con A integralmente chiuso e B intero su A. Siano $\mathfrak{p}_1 \supseteq \dots \supseteq \mathfrak{p}_n$ una catena di ideali primi di A, e $\mathfrak{q}_1 \supseteq \dots \supseteq \mathfrak{q}_m$ $(m < n)$ una catena di ideali primi di B tali che $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ $(1 \leq i \leq m)$. Allora la catena $\mathfrak{q}_1 \supseteq \dots \supseteq \mathfrak{q}_m$ può essere estesa ad una catena $\mathfrak{q}_1 \supseteq \dots \supseteq \mathfrak{q}_n$ tale che $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ $(1 \leq i \leq n)$.*

Dimostrazione. Come si è visto in (5.11), ci si riduce immediatamente al caso in cui $m = 1$, $n = 2$. Allora occorre provare che $\mathfrak{p}_2$ è la contrazione di un ideale primo dell'anello $B_{\mathfrak{q}_1}$, o in modo equivalente (cfr. (3.16)) che $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$.

Ogni elemento $x \in B_{\mathfrak{q}_1}\mathfrak{p}_2$ è della forma y/s, dove $y \in B\mathfrak{p}_2$ e $s \in B - \mathfrak{q}_1$. In virtú di (5.14), y è intero su $\mathfrak{p}_2$, e quindi, stante (5.15), la sua equazione di grado minimo su K, il campo delle frazioni di A, è della forma

$$y^r + u_1 y^{r-1} + \dots + u_r = 0 \tag{1}$$

con $u_1, \dots, u_r$ in $\mathfrak{p}_2$.

Supponiamo ora che $x \in B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$. Allora $s = yx^{-1}$ con $x^{-1} \in K$, cosicché l'equazione di grado minimo per s su K si ottiene dividendo la (1) per x^r, e si ha, diciamo,

$$s^r + v_1 s^{r-1} + \dots + v_r = 0 \tag{2}$$

dove $v_i = u_i/x^i$. Di conseguenza

$$x^i v_i = u_i \in \mathfrak{p}_2 \qquad (1 \leq i \leq r). \tag{3}$$

Ma s è intero su A, dunque, in virtú di (5.15) (con $\mathfrak{a} = (1)$) ciascun v_i appartiene ad A. Supponiamo che $x \notin \mathfrak{p}_2$. Allora la (3) mostra che ciascun $v_i \in \mathfrak{p}_2$, da cui, stante la (2), $s^r \in B\mathfrak{p}_2 \subseteq B\mathfrak{p}_1 \subseteq \mathfrak{q}_1$, e quindi $s \in \mathfrak{q}_1$, ciò che è una contraddizione. Ne segue che $x \in \mathfrak{p}_2$ e pertanto $B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A = \mathfrak{p}_2$, come richiesto. ■

La dimostrazione della proposizione seguente presuppone alcuni risultati classici della teoria dei campi.

Proposizione 5.17. *Sia A un dominio di integrità integralmente chiuso e K il suo campo delle frazioni, sia L un'estensione algebrica finita separabile di K e B la chiusura integrale di A in L. Allora esiste una base $v_1, \ldots, v_n$ di L su K tale che $B \subseteq \sum_{j=1}^{n} Av_j$.*

Dimostrazione. Se v è un elemento arbitrario di L, allora v è algebrico su K e pertanto soddisfa ad un'equazione della forma

$$a_0v^r + a_1v^{r-1} + \qquad + a_n = 0 \qquad (a_i \in A).$$

Moltiplicando tale equazione per a_0^{r-1}, si vede che $a_0v = u$ è intero su A, e quindi appartiene a B. Dunque, data una qualsiasi base di L su K, è possibile moltiplicare gli elementi della base per opportuni elementi di A, in modo da ottenere una base $u_1, \ldots, u_n$ tale che ciascun $u_i \in B$.

Denotiamo con T la traccia (da L a K). Poiché L/K è separabile, la forma bilineare $(x, y) \mapsto T(xy)$ su L (considerato come spazio vettoriale su K) è non degenere, e quindi si ottiene una base duale $v_1, \ldots, v_n$ di L su K, definita da $T(u_iv_j) = \delta_{ij}$. Sia x un elemento arbitrario di B, diciamo $x = \sum_j x_jv_j\,(x_j \in K)$. Si ha $xu_i \in B$ (giacché $u_i \in B$) e pertanto $T(xu_i) \in A$, in virtú di (5.15) (poiché la traccia di un elemento è un multiplo di uno dei coefficienti del polinomio minimo). Ma $T(xu_i) = \sum_j T(x_ju_iv_j) = \sum_j x_jT(u_iv_j) = \sum_j x_j\delta_{ij} = x_i$, dunque $x_i \in A$. Di conseguenza, $B \subseteq \sum_j Av_j$. ■

Anelli di valutazione

Sia B un dominio di integrità, K il suo campo delle frazioni. Si dice che B è un *anello di valutazione* di K se, per ogni elemento $x \neq 0$ in K, o $x \in B$ oppure $x^{-1} \in B$ (le due eventualità potendosi presentare simultaneamente).

Proposizione 5.18. i) *B è un anello locale.*

ii) *Se B' è un anello tale che $B \subseteq B' \subseteq K$, allora B' è un anello di valutazione di K.*

iii) *B è integralmente chiuso (in K).*

Dimostrazione. i) Sia $\mathfrak{m}$ l'insieme degli elementi non invertibili di B, sicché $x \in \mathfrak{m} \Leftrightarrow x = 0$ oppure $x^{-1} \notin B$. Se $a \in B$ e $x \in \mathfrak{m}$ si ha $ax \in \mathfrak{m}$, giacché altrimenti $(ax)^{-1} \in B$ e pertanto $x^{-1} = a\,(ax)^{-1} \in B$. Siano poi x, y elementi non nulli di $\mathfrak{m}$. Allora o $xy^{-1} \in B$ oppure $x^{-1}y \in B$. Se $xy^{-1} \in B$ allora $x + y = (1 + xy^{-1})\,y \in B\mathfrak{m} \subseteq \mathfrak{m}$, e similmente se $x^{-1}y \in B$. Dunque $\mathfrak{m}$ è un ideale e pertanto B è un anello locale, in virtú di (1.6).

ii) segue chiaramente dalle definizioni.

iii) Sia $x \in K$ intero su B. Allora si ha, diciamo,

$$x^n + b_1x^{n-1} + \cdots + b_n = 0$$

con i $b_i \in B$. Se $x \in B$, non c'è nulla da dimostrare. Altrimenti, si ha $x^{-1} \in B$, da cui $x = -(b_1 + b_2x^{-1} + \cdots + b_nx^{1-n}) \in B$. ∎

Sia K un campo, Ω un campo algebricamente chiuso. Sia Σ l'insieme di tutte le coppie (A, f), dove A è un subanello di K e f è un omomorfismo di A in Ω. Introduciamo una relazione di ordine parziale in Σ nel modo seguente:

$$(A, f) \leqslant (A', f') \Leftrightarrow A \subseteq A' \text{ e } f'|_A = f.$$

Le condizioni del lemma di Zorn sono chiaramente soddisfatte e pertanto l'insieme Σ possiede almeno un elemento massimale.

Sia (B, g) un elemento massimale di Σ. Vogliamo provare che B è un anello di valutazione di K. Il primo passo nella dimostrazione è il:

Lemma 5.19. *B è un anello locale e $\mathfrak{m} = \operatorname{Ker}(g)$ è il suo ideale massimale.*

Dimostrazione. Poiché $g(B)$ è un subanello di un campo e quindi un dominio di integrità, l'ideale $\mathfrak{m} = \operatorname{Ker}(g)$ è primo. Possiamo estendere g ad un omomorfismo $\bar{g}\colon B_\mathfrak{m} \to \Omega$, ponendo $\bar{g}(b/s) = g(b)/g(s)$ per ogni $b \in B$ e per ogni $s \in B - \mathfrak{m}$, giacché certamente $g(s) \neq 0$. Poiché la coppia (B, g) è massimale, si ha che $B = B_\mathfrak{m}$; dunque B è un anello locale e $\mathfrak{m}$ è il suo ideale massimale. ∎

Lemma 5.20. *Sia x un elemento non nullo di K. Sia $B[x]$ il subanello di K generato da x sopra B, e $\mathfrak{m}[x]$ l'estensione di $\mathfrak{m}$ in $B[x]$. Allora o $\mathfrak{m}[x] \neq B[x]$ oppure $\mathfrak{m}[x^{-1}] \neq B[x^{-1}]$.*

Dimostrazione. Supponiamo che $\mathfrak{m}[x] = B[x]$ e $\mathfrak{m}[x^{-1}] = B[x^{-1}]$. Allora si avranno equazioni

$$(1) \qquad u_0 + u_1 x + \quad + u_m x^m = 1 \qquad (u_i \in \mathfrak{m})$$

$$(2) \qquad v_0 + v_1 x^{-1} + \quad + v_n x^{-n} = 1 \qquad (v_j \in \mathfrak{m})$$

e non è restrittivo supporre che entrambe siano di grado minimo. Supponiamo che $m \geqslant n$, e moltiplichiamo la (2) per x^n:

$$(3) \qquad (1 - v_0)x^n = v_1 x^{n-1} + \quad + v_n.$$

Poiché $v_0 \in \mathfrak{m}$, segue da (5.19) che $1 - v_0$ è invertibile in B, e pertanto la (3) può riscriversi nella forma

$$x^n = w_1 x^{n-1} + \quad + w_n \qquad (w_j \in \mathfrak{m}).$$

Dunque si può sostituire x^m nella (1) con $w_1 x^{m-1} + \quad + w_n x^{m-n}$, e ciò contraddice la minimalità dell'esponente m. ■

Teorema 5.21. *Sia (B, g) un elemento massimale di Σ. Allora B è un anello di valutazione del campo K.*

Dimostrazione. Occorre provare che se $x \neq 0$ è un elemento di K, allora o $x \in B$ oppure $x^{-1} \in B$. In virtù di (5.20), possiamo supporre che $\mathfrak{m}[x]$ non è l'ideale unità dell'anello $B' = B[x]$. Allora $\mathfrak{m}[x]$ è contenuto in un ideale massimale $\mathfrak{m}'$ di B', e si ha $\mathfrak{m}' \cap B = \mathfrak{m}$ (poiché $\mathfrak{m}' \cap B$ è un ideale proprio di B e contiene $\mathfrak{m}$). Dunque l'immersione di B in B' induce un'immersione del campo $k = B/\mathfrak{m}$ nel campo $k' = B'/\mathfrak{m}'$; inoltre $k' = k[\bar{x}]$ dove $\bar{x}$ è l'immagine di x in k', sicché $\bar{x}$ è algebrico su k e pertanto k' è un'estensione algebrica finita di k.

Ora l'omomorfismo g induce un'immersione $\bar{g}$ di k in Ω, giacché (cfr. (5.19)) $\mathfrak{m}$ è il nucleo di g. Poiché Ω è algebricamente chiuso, $\bar{g}$ può essere esteso ad una immersione $\bar{g}'$ di k' in Ω. Componendo $\bar{g}'$ con l'omomorfismo naturale $B' \to k'$, si ottiene un omomorfismo, diciamo $g'\colon B' \to \Omega$ che estende g. Ma la coppia (B, g) è massimale, dunque $B' = B$ e pertanto $x \in B$. ■

Corollario 5.22. *Sia A un subanello di un campo K. Allora la chiusura integrale $\bar{A}$ di A in K è l'intersezione di tutti gli anelli di valutazione di K che contengono A.*

Dimostrazione. Sia B un anello di valutazione di K tale che $A \subseteq B$. Poiché B è integralmente chiuso, in virtú di (5.18) iii), si ha che $\bar{A} \subseteq B$.

Viceversa, sia x un arbitrario elemento di K tale che $x \notin \bar{A}$. Allora x non appartiene all'anello $A' = A[x^{-1}]$. Dunque x^{-1} non è invertibile in A' e pertanto è contenuto in un ideale massimale $\mathfrak{m}'$ di A'. Sia Ω una chiusura algebrica del campo $k' = A'/\mathfrak{m}'$. Allora la restrizione ad A dell'omomorfismo naturale $A' \to k'$ definisce un omomorfismo di A in Ω. In virtú di (5.21), esso può essere esteso a qualche anello di valutazione $B \supseteq A$. Ma allora, poiché x^{-1} viene mandato nello zero, ne segue che $x \notin B$. ■

Proposizione 5.23. *Siano $A \subseteq B$ domini di integrità, con B finitamente generato su A. Sia v un elemento non nullo di B. Allora esiste un elemento $u \neq 0$ in A con la seguente proprietà: ogni omomorfismo f di A in un campo algebricamente chiuso Ω tale che $f(u) \neq 0$ può essere esteso ad un omomorfismo g di B in Ω tale che $g(v) \neq 0$.*

Dimostrazione. Procedendo per induzione sul numero dei generatori di B sopra A, ci si riduce immediatamente al caso in cui B è generato su A da un solo elemento x.

i) Supponiamo che x sia trascendente su A, ossia, x non è radice di alcun polinomio non nullo a coefficienti in A. Sia $v = a_0x^n + a_1x^{n-1} + \cdots + a_n$ e prendiamo $u = a_0$. Ora se $f: A \to \Omega$ è tale che $f(u) \neq 0$, esiste un elemento $\xi \in \Omega$ tale che $f(a_0)\xi^n + f(a_1)\xi^{n-1} + \cdots + f(a_n) \neq 0$, poiché Ω è infinito. Estendiamo poi f ad un omomorfismo $g: B \to \Omega$ definito ponendo $g(x) = \xi$. Allora $g(v) \neq 0$, come richiesto.

ii) Supponiamo ora che x sia algebrico su A (ossia sul campo delle frazioni di A). Allora tale risulta v^{-1}, poiché v è un polinomio in x. Dunque si hanno equazioni della forma

$$(1) \qquad a_0x^m + a_1x^{m-1} + \cdots + a_m = 0 \qquad (a_i \in A)$$

$$(2) \qquad a_0'v^{-n} + a_1'v^{1-n} + \cdots + a_n' = 0 \qquad (a_j' \in A).$$

Poniamo $u = a_0a_0'$, e sia $f: A \to \Omega$ tale che $f(u) \neq 0$. Allora f può essere esteso innanzitutto ad un omomorfismo $f_1: A[u^{-1}] \to \Omega$ (con $f_1(u^{-1}) = f(u)^{-1}$), e successivamente, in virtú di (5.21), ad un omomorfismo $h: C \to \Omega$, dove C è un anello di valutazione contenente $A[u^{-1}]$. Stante la (1), x è intero su $A[u^{-1}]$, e quindi (cfr. (5.22)) $x \in C$, sicché C contiene B, e in particolare $v \in C$. D'altra parte, dalla (2) si ha che v^{-1} è intero su $A[u^{-1}]$, e pertanto appartiene a C, ancora in virtú di

(5.22). Dunque v è invertibile in C, e quindi $h(v) \neq 0$. A questo punto, per concludere, basta definire g come la restrizione di h a B. ■

Corollario 5.24. *Sia k un campo e B una k-algebra finitamente generata. Se B è un campo, allora B risulta un'estensione algebrica finita di k.*

Dimostrazione. Basta prendere $A = k$, $v = 1$ e $\Omega =$ chiusura algebrica di k. ■

L'enunciato (5.24) è una delle forme del *Nullstellensatz* o Teorema degli zeri di Hilbert. Per un'altra dimostrazione, cfr. (7.9).

Esercizi

1. Sia $f\colon A \to B$ un omomorfismo intero di anelli. Provare che $f^*\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ è un'applicazione *chiusa*, ossia manda sottoinsiemi chiusi in sottoinsiemi chiusi. (Si tratta di una formulazione geometrica equivalente di (5.10).)
2. Sia A un subanello di un anello B tale che B è intero su A, e sia $f\colon A \to \Omega$ un omomorfismo di A in un campo algebricamente chiuso Ω. Dimostrare che f può essere esteso ad un omomorfismo di B in Ω. [Utilizzare (5.10).]
3. Sia $f\colon B \to B'$ un omomorfismo di A-algebre, e sia C una A-algebra. Se f è intero, provare che $f \otimes 1\colon B \otimes_A C \to B' \otimes_A C$ è intero. (Tale risultato include (5.6) ii) come caso particolare.)
4. Sia A un subanello di un anello B tale che B è intero su A. Sia $\mathfrak{n}$ un ideale massimale di B e sia $\mathfrak{m} = \mathfrak{n} \cap A$ l'ideale massimale corrispondente di A. È vero che $B_\mathfrak{n}$ risulta necessariamente intero su $A_\mathfrak{m}$?
   [Consideriamo il subanello $k[x^2 - 1]$ di $k[x]$, dove k è un campo, e sia $\mathfrak{n} = (x - 1)$. Può l'elemento $1/(x + 1)$ essere intero?]
5. Siano $A \subseteq B$ anelli, con B intero su A.
   i) Se $x \in A$ è invertibile in B, allora risulta invertibile in A.
   ii) Il radicale di Jacobson di A è la contrazione del radicale di Jacobson di B.
6. Siano $B_1, \ldots, B_n$ A-algebre intere. Dimostrare che $\prod_{i=1}^{n} B_i$ è una A-algebra intera.
7. Sia A un subanello di un anello B, tale che l'insieme $B - A$ è chiuso rispetto alla moltiplicazione. Provare che A è integralmente chiuso in B.

8. i) Sia A un subanello di un dominio di integrità B, e sia C la chiusura integrale di A in B. Siano f, g polinomi monici in $B[x]$ tali che $fg \in C[x]$. Allora f e g appartengono a $C[x]$. [Prendiamo un campo contenente B in cui i polinomi f, g si spezzano in fattori lineari: diciamo $f = \Pi\,(x - \xi_i)$, $g = \Pi\,(x - \eta_j)$. Ciascun ξ_i e ciascun η_j è una radice di fg, dunque è intero su C. Ne segue che i coefficienti di f e di g sono interi su C.]

   ii) Dimostrare lo stesso risultato senza supporre che B (oppure A) è un dominio di integrità.

9. Sia A un subanello di un anello B e sia C la chiusura integrale di A in B. Provare che $C[x]$ è la chiusura integrale di $A[x]$ in $B[x]$. [Se $f \in B[x]$ è intero su $A[x]$, allora

$$f^m + g_1 f^{m-1} + \quad + g_m = 0 \qquad (g_i \in A[x]).$$

Sia r un intero maggiore di m e dei gradi di $g_1, \ldots, g_m$, e poniamo $f_1 = f - x^r$, sicché

$$(f_1 + x^r)^m + g_1(f + x^r)^{m-1} + \quad + g_m = 0$$

ossia, diciamo

$$f_1^m + h_1 f_1^{m-1} + \quad + h_m = 0,$$

dove $h_m = (x^r)^m + g_1(x^r)^{m-1} + \ldots + g_m \in A[x]$. Ora basta applicare l'Esercizio 8 ai polinomi $-f_1$ e $f_1^{m-1} + h_1 f_1^{m-2} + \quad + h_{m-1}$.]

10. Si dice che un omomorfismo di anelli $f\colon A \to B$ possiede la *proprietà del going-up* (risp. la *proprietà del going-down*) se la tesi del teorema del going-up (5.11) (risp. del teorema del going-down (5.16)) vale per B e il suo subanello $f(A)$.

    Sia $f^*\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ l'applicazione associata a f.

    i) Consideriamo le tre affermazioni seguenti:

    (a) f^* è un'applicazione chiusa.

    (b) f possiede la proprietà del going-up.

    (c) Sia $\mathfrak{q}$ un ideale primo arbitrario di B e $\mathfrak{p} = \mathfrak{q}^c$. Allora $f^*\colon \operatorname{Spec}(B/\mathfrak{q}) \to \operatorname{Spec}(A/\mathfrak{p})$ è suriettiva.

    Dimostrare che (a) $\Rightarrow$ (b) $\Leftrightarrow$ (c). (Cfr. anche Capitolo 6, Esercizio 11.)

    ii) Consideriamo le tre affermazioni seguenti:

    (a′) f^* è un'applicazione aperta.

    (b′) f possiede la proprietà del going-down.

(c') Sia $\mathfrak{q}$ un ideale primo arbitrario di B e $\mathfrak{p} = \mathfrak{q}^c$. Allora f^*: $\operatorname{Spec}(B_\mathfrak{q}) \to \operatorname{Spec}(A_\mathfrak{p})$ è suriettiva.

Dimostrare che $(a') \Rightarrow (b') \Leftrightarrow (c')$. (Cfr. anche Capitolo 7, Esercizio 24.)

[Per provare che $(a') \Rightarrow (c')$, osserviamo che $B_\mathfrak{q}$ è il limite diretto degli anelli B_t, dove $t \in B - \mathfrak{q}$; dunque, in virtú dell'Esercizio 26 del Capitolo 3, si ha che $f^*(\operatorname{Spec}(B_\mathfrak{q})) = \bigcap_t f^*(\operatorname{Spec}(B_t)) = \bigcap_t f^*(Y_t)$, essendo $Y = \operatorname{Spec}(B)$. Poiché Y_t è un intorno aperto di $\mathfrak{q}$ in Y, e inoltre f^* è aperta, ne segue che $f^*(Y_t)$ è un intorno aperto di $\mathfrak{p}$ in $\operatorname{Spec}(A)$ e pertanto contiene $\operatorname{Spec}(A_\mathfrak{p})$.]

11. Sia $f: A \to B$ un omomorfismo piatto di anelli. Allora f possiede la proprietà del going-down. [Cfr. Capitolo 3, Esercizio 18.]

12. Sia G un gruppo finito di automorfismi di un anello A, e denotiamo con A^G il subanello dei G-invarianti, ossia di tutti gli elementi $x \in A$ tali che $\sigma(x) = x$ per ogni $\sigma \in G$. Dimostrare che A è intero su A^G. [Basta osservare che ogni elemento $x \in A$ è una radice del polinomio $\prod_{\sigma \in G}(t - \sigma(x))$.]

    Sia S una parte moltiplicativa di A tale che $\sigma(S) \subseteq S$ per ogni $\sigma \in G$, e poniamo $S^G = S \cap A^G$. Provare che l'azione di G su A si estende ad un'azione su $S^{-1}A$, e che $(S^G)^{-1}A^G \cong (S^{-1}A)^G$.

13. Nella situazione dell'Esercizio 12, sia $\mathfrak{p}$ un ideale primo di A^G, e sia P l'insieme degli ideali primi di A la cui contrazione è $\mathfrak{p}$. Dimostrare che G agisce transitivamente su P. In particolare, P è *finito*. [Siano $\mathfrak{p}_1, \mathfrak{p}_2 \in P$ e sia $x \in \mathfrak{p}_1$. Allora $\prod_\sigma \sigma(x) \in \mathfrak{p}_1 \cap A^G = \mathfrak{p} \subseteq \mathfrak{p}_2$, da cui $\sigma(x) \in \mathfrak{p}_2$ per qualche $\sigma \in G$. Dedurre che $\mathfrak{p}_1$ è contenuto nell'unione $\bigcup_{\sigma \in G} \sigma(\mathfrak{p}_2)$, e applicare poi (1.11) e (5.9).]

14. Sia A un dominio di integrità integralmente chiuso, K il suo campo delle frazioni e L un'estensione finita normale separabile di K. Sia G il gruppo di Galois di L su K e sia B la chiusura integrale di A in L. Provare che $\sigma(B) = B$ per ogni $\sigma \in G$, e inoltre che $A = B^G$.

15. Siano A e K come nell'Esercizio 14, sia L un'arbitraria estensione finita di K, e sia B la chiusura integrale di A in L. Dimostrare che, se $\mathfrak{p}$ è un ideale primo qualsiasi di A, allora l'insieme degli ideali primi $\mathfrak{q}$ di B che si contraggono a $\mathfrak{p}$ è finito (in altre parole, che l'applicazione $\operatorname{Spec}(B) \to \operatorname{Spec}(A)$ ha fibre finite).
    [Ridursi ai due casi (a) L separabile su K e (b) L puramente inse-

parabile su K. Nel caso (a), immergere L in un'estensione finita normale separabile di K, e utilizzare gli Esercizi 13 e 14. Nel caso (b), se $\mathfrak{q}$ è un ideale primo di B tale che $\mathfrak{q} \cap A = \mathfrak{p}$, provare che $\mathfrak{q}$ è l'insieme di tutti gli elementi $x \in B$ tali che $x^{p^m} \in \mathfrak{p}$ per qualche $m \geqslant 0$, dove p è la caratteristica di K, e quindi che l'applicazione $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ è biiettiva, nelle ipotesi attuali.]

Il lemma di normalizzazione di Noether

16. Sia k un campo e sia $A \neq 0$ una k-algebra finitamente generata. Allora esistono elementi $y_1, \ldots, y_r \in A$ che sono algebricamente indipendenti su k e tali che A è intero su $k[y_1, \ldots, y_r]$.

    Supponiamo che k sia *infinito*. (Il risultato è ancora vero se k è finito, ma richiede una dimostrazione diversa.) Siano $x_1, \ldots, x_n$ un sistema di generatori di A come k-algebra. Possiamo rinumerare gli x_i in modo tale che $x_1, \ldots, x_r$ siano algebricamente indipendenti su k e ciascuno degli elementi $x_{r+1}, \ldots, x_n$ sia algebrico su $k[x_1, \ldots, x_r]$. Procediamo ora per induzione rispetto a n. Se $n = r$, non c'è nulla da dimostrare, sicché supponiamo $n > r$ e il risultato vero per $n - 1$ generatori. Il generatore x_n è algebrico su $K[x_1, \ldots, x_{n-1}]$, dunque esiste un polinomio $f \neq 0$ in n variabili tale che $f(x_1, \quad , x_{n-1}, x_n) = 0$. Sia F il termine omogeneo di grado più alto in f. Poiché k è infinito, esistono elementi $\lambda_1, \ldots, \lambda_{n-1} \in k$ tali che $F(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$. Poniamo $x'_i = x_i - \lambda_i x_n$ $(1 \leqslant i \leqslant n-1)$. Dimostrare che x_n è intero sull'anello $A' = k[x'_1, \ldots, x'_{n-1}]$, e quindi che A è intero su A'. A questo punto, basta applicare l'ipotesi induttiva ad A' per completare la dimostrazione.

    Dalla dimostrazione segue che $y_1, \ldots, y_r$ possono essere scelti come combinazioni lineari di $x_1, \ldots, x_n$. Ciò ha la seguente interpretazione geometrica: se k è algebricamente chiuso e X è una varietà algebrica affine in k^n con anello delle coordinate $A \neq 0$, allora esiste un sottospazio lineare L di dimensione r in k^n ed un'applicazione lineare di k^n su L che manda X *sopra* L. [Utilizzare l'Esercizio 2.]

Il teorema degli zeri di Hilbert (forma debole)

17. Sia $\mathfrak{a} \neq (1)$ un ideale nell'anello dei polinomi $k[t_1, \ldots, t_n]$, essendo k un campo algebricamente chiuso. Allora l'insieme $V(\mathfrak{a})$ dei

punti $x = (x_1, \ldots, x_n) \in k^n$ tali che $f(x) = 0$ per ogni $f \in \mathfrak{a}$, è non vuoto.
[Poniamo $A = k[t_1, \ldots, t_n]/\mathfrak{a}$. Allora $A \neq 0$, sicché in virtú dell'Esercizio 16, esiste un sottospazio lineare L di dimensione $\geqslant 0$ in k^n ed un'applicazione di $V(\mathfrak{a})$ *sopra* L. Dunque $V(\mathfrak{a}) \neq \emptyset$.]

Dedurre che ogni ideale massimale nell'anello $k[t_1, \ldots, t_n]$ è della forma $(t_1 - a_1, \ldots, t_n - a_n)$ dove $a_i \in k$.

18. Sia k un campo e sia B una k-algebra finitamente generata. Supponiamo che B sia un campo. Allora B è un'estensione algebrica finita di k. (Questa è un'altra versione del Teorema degli zeri di Hilbert. La dimostrazione seguente è dovuta a Zariski. Per altre dimostrazioni, cfr. (5.24), (7.9).)

Siano $x_1, \ldots, x_n$ un sistema di generatori di B come k-algebra. Si procede per induzione su n. Se $n = 1$, il risultato è banalmente vero, sicché supponiamo $n > 1$. Poniamo $A = k[x_1]$ e sia $K = k(x_1)$ il campo delle frazioni di A. In virtú dell'ipotesi induttiva, B è un'estensione algebrica finita di K, dunque ciascuno degli elementi $x_2, \ldots, x_n$ soddisfa ad un'equazione polinomiale monica a coefficienti in K, ossia a coefficienti della forma a/b, dove a e b appartengono ad A. Se f è il prodotto dei denominatori di tutti questi coefficienti, allora ciascuno degli elementi $x_2, \ldots, x_n$ è intero su A_f. Dunque B, e di conseguenza K, è intero su A_f.

Supponiamo che x_1 sia trascendente su k. Allora A è integralmente chiuso, poiché è un dominio a fattorizzazione unica. Dunque A_f è integralmente chiuso (cfr. (5.12)), e pertanto $A_f = K$, ciò che chiaramente è assurdo. Ne segue che x_1 è algebrico su k, sicché K (e di conseguenza B) è un'estensione finita di k.

19. Dedurre il risultato dell'Esercizio 17 dall'Esercizio 18.

20. Sia A un subanello di un dominio di integrità B tale che B è una A-algebra finitamente generata. Dimostrare che esistono un elemento $s \neq 0$ in A ed elementi $y_1, \ldots, y_n$ in B, algebricamente indipendenti su A, tali che B_s è intero su B'_s, dove $B' = A[y_1, \ldots, y_n]$. [Sia $S = A - \{0\}$ e $K = S^{-1}A$, il campo delle frazioni di A. Allora $S^{-1}B$ è una K-algebra finitamente generata e pertanto, in virtú del lemma di normalizzazione (Esercizio 16), esistono elementi $x_1, \ldots, x_n$ in $S^{-1}B$, algebricamente indipendenti su K e tali che $S^{-1}B$ è intero su $K[x_1, \ldots, x_n]$. Siano $z_1, \ldots, z_m$ un sistema di generatori di B come A-algebra. Allora ciascun z_j (considerato come elemento di $S^{-1}B$) è intero su $K[x_1, \ldots, x_n]$. Scrivendo un'equazione di dipendenza integrale per ciascun z_j,

dimostrare che esiste un elemento $s \in S$ tale che $x_i = y_i/s$ ($1 \leqslant i \leqslant n$) con $y_i \in B$, e tale inoltre che ciascun elemento sz_j è intero su B'. Dedurre che un siffatto elemento s soddisfa le condizioni richieste.]

21. Siano A e B come nell'Esercizio 20. Provare che esiste un elemento $s \neq 0$ in A tale che, se Ω è un campo algebricamente chiuso e $f: A \to \Omega$ è un omomorfismo per il quale $f(s) \neq 0$, allora f può essere esteso ad un omomorfismo $B \to \Omega$. [Con le notazioni dell'Esercizio 20, f può essere esteso innanzitutto a B', per esempio mandando ciascun y_i in 0, poi a B'_s (giacché $f(s) \neq 0$), e infine a B_s (in virtú dell'Esercizio 2, poiché B_s è intero su B'_s).]

22. Siano A e B come nell'Esercizio 20. Se il radicale di Jacobson di A è zero, allora tale risulta il radicale di Jacobson di B. [Sia $v \neq 0$ un elemento di B. Occorre provare che esiste un ideale massimale di B che non contiene v. Applicando l'Esercizio 21 all'anello B_v e al suo subanello A, si ottiene un elemento $s \neq 0$ in A. Sia $\mathfrak{m}$ un ideale massimale di A tale che $s \notin \mathfrak{m}$, e poniamo $k = A/\mathfrak{m}$. Allora l'applicazione canonica $A \to k$ si estende ad un omomorfismo g di B_v in una chiusura algebrica Ω di k. Provare che $g(v) \neq 0$ e che $\operatorname{Ker}(g) \cap B$ è un ideale massimale di B.]

23. Sia A un anello. Dimostrare che le seguenti affermazioni sono equivalenti:
    i) Ogni ideale primo di A è un'intersezione di ideali massimali.
    ii) In ogni immagine omomorfa di A il nilradicale è uguale al radicale di Jacobson.
    iii) Ogni ideale primo di A, che non sia massimale, è uguale all'intersezione degli ideali primi che lo contengono propriamente.

    [L'unica implicazione non banale è iii) $\Rightarrow$ ii). Supponiamo che ii) non sia vera; allora esiste un ideale primo che non è un'intersezione di ideali massimali. Passando all'anello quoziente, possiamo supporre che A è un dominio di integrità il cui radicale di Jacobson $\mathfrak{R}$ è non nullo. Sia f un elemento non nullo di $\mathfrak{R}$. Allora $A_f \neq 0$, sicché A_f possiede un ideale massimale, la cui contrazione in A è un ideale primo $\mathfrak{p}$ tale che $f \notin \mathfrak{p}$, e che è massimale rispetto a tale proprietà. Allora $\mathfrak{p}$ non è massimale e non è uguale all'intersezione degli ideali primi che contengono propriamente $\mathfrak{p}$.]

    Un anello A con le tre proprietà equivalenti di cui sopra prende il nome di *anello di Jacobson*.

24. Sia A un anello di Jacobson (Esercizio 23) e B una A-algebra. Dimostrare che se (i) B è intero su A oppure (ii) B è una A-algebra finitamente generata, allora B è un anello di Jacobson. [Utilizzare l'Esercizio 22 per (ii).]

    In particolare, ogni anello finitamente generato, e ogni algebra finitamente generata sopra un campo, è un anello di Jacobson.

25. Sia A un anello. Provare che le seguenti condizioni sono equivalenti:

    i) A è un anello di Jacobson;

    ii) Ogni A-algebra finitamente generata B che sia un campo, risulta finita su A.

    [i) $\Rightarrow$ ii). Ci riduciamo al caso in cui A è un subanello di B, e utilizziamo l'Esercizio 21. Se s è un elemento di A con le proprietà enunciate nell'Esercizio 21, allora esiste un ideale massimale $\mathfrak{m}$ di A che non contiene s, e l'omomorfismo $A \to A/\mathfrak{m} = k$ si estende ad un omomorfismo g di B nella chiusura algebrica di k. Poiché B è un campo, g è iniettivo, e $g(B)$ è un'estensione algebrica di k, dunque un'estensione algebrica finita di k.
    ii) $\Rightarrow$ i). Utilizziamo il criterio iii) dell'Esercizio 23. Sia $\mathfrak{p}$ un ideale primo di A non massimale, e poniamo $B = A/\mathfrak{p}$. Sia f un elemento non nullo di B. Allora B_f è una A-algebra finitamente generata. Se B_f è un campo, essa è finita su B, dunque intera su B e pertanto B è un campo, in virtú di (5.7). Ne segue che B_f non è un campo e pertanto possiede un ideale primo non nullo, la cui contrazione in B è un ideale non nullo $\mathfrak{p}'$ tale che $f \notin \mathfrak{p}'$.]

26. Sia X uno spazio topologico. Un sottoinsieme di X è *localmente chiuso* se è l'intersezione di un aperto e di un chiuso, o in modo equivalente, se è aperto nella sua chiusura.

    Le seguenti condizioni su un sottoinsieme X_0 di X sono equivalenti:

    (1) Ogni sottoinsieme non vuoto localmente chiuso di X interseca X_0;

    (2) Per ogni chiuso E di X si ha $\overline{E \cap X_0} = E$;

    (3) L'applicazione $U \mapsto U \cap X_0$ dell'insieme degli aperti di X sull'insieme degli aperti di X_0 è *biiettiva*.

    Un sottoinsieme X_0 che soddisfa tali condizioni si dice *molto denso* in X.

    Se A è un anello, provare che le seguenti affermazioni sono equivalenti:

i) A è un anello di Jacobson;

ii) L'insieme degli ideali massimali di A è molto denso in Spec (A);

iii) Ogni sottoinsieme localmente chiuso di Spec (A) costituito da un solo punto è chiuso.

[ii) e iii) sono formulazioni geometriche delle condizioni ii) e iii) dell'Esercizio 23.]

Anelli di valutazione e valutazioni

27. Siano A, B due anelli locali. Si dice che B *domina* A, se A è un subanello di B e l'ideale massimale $\mathfrak{m}$ di A è contenuto nell'ideale massimale $\mathfrak{n}$ di B (o in modo equivalente, se $\mathfrak{m} = \mathfrak{n} \cap A$). Sia K un campo e sia Σ l'insieme di tutti i subanelli locali di K. Se Σ è ordinato rispetto alla relazione di dominanza, provare che Σ possiede elementi massimali e che $A \in \Sigma$ è massimale se e soltanto se A è un anello di valutazione di K.
[Utilizzare (5.20).]

28. Sia A un dominio di integrità, K il suo campo delle frazioni. Dimostrare che le seguenti condizioni sono equivalenti:

   (1) A è un anello di valutazione di K;

   (2) Se $\mathfrak{a}$, $\mathfrak{b}$ sono due ideali arbitrari di A, allora o $\mathfrak{a} \subseteq \mathfrak{b}$, oppure $\mathfrak{b} \subseteq \mathfrak{a}$.

   Dedurre che, se A è un anello di valutazione e $\mathfrak{p}$ è un ideale primo di A, allora $A_{\mathfrak{p}}$ e $A/\mathfrak{p}$ sono anelli di valutazione dei loro campi di frazioni.

29. Sia A un anello di valutazione di un campo K. Dimostrare che ogni subanello di K che contiene A è un anello locale di A.

30. Sia A un anello di valutazione di un campo K. Il gruppo U degli elementi invertibili di A è un sottogruppo del gruppo moltiplicativo K^* di K.

   Poniamo $\Gamma = K^*/U$. Se $\xi, \eta \in \Gamma$ sono rappresentati da x, $y \in K$, definiamo $\xi \geqslant \eta$ per significare che $xy^{-1} \in A$. Dimostrare che ciò definisce un ordinamento totale in Γ che è compatibile con la struttura di gruppo (ossia, $\xi \geqslant \eta \Rightarrow \xi\omega \geqslant \eta\omega$ per ogni $\omega \in \Gamma$). In altre parole, Γ è un gruppo abeliano totalmente ordinato. Esso è chiamato il *gruppo dei valori* di A.

Sia $v: K^* \to \Gamma$ l'omomorfismo canonico. Dimostrare che $v(x + y) \geq \min(v(x), v(y))$ per ogni $x, y \in K^*$.

31. Viceversa, sia Γ un gruppo abeliano totalmente ordinato (scritto *additivamente*), e sia K un campo. Una *valutazione di K a valori in Γ* è un'applicazione $v: K^* \to \Gamma$ tale che:

    (1) $v(xy) = v(x) + v(y)$,

    (2) $v(x + y) \geq \min(v(x), v(y))$,

    per ogni $x, y \in K^*$. Dimostrare che l'insieme degli elementi $x \in K^*$ tali che $v(x) \geq 0$, insieme allo zero, è un anello di valutazione di K. Tale anello prende il nome di *anello di valutazione* di v, e il sottogruppo $v(K^*)$ di Γ è il *gruppo dei valori* di v.

    Dunque le nozioni di anello di valutazione e di valutazione sono essenzialmente equivalenti.

32. Sia Γ un gruppo abeliano totalmente ordinato. Un sottogruppo Δ di Γ è *isolato* in Γ se, ogni volta che $0 \leq \beta \leq \alpha$ e $\alpha \in \Delta$, si ha $\beta \in \Delta$. Sia A un anello di valutazione di un campo K, con gruppo dei valori Γ (Esercizio 31). Se $\mathfrak{p}$ è un ideale primo di A, provare che $v(A - \mathfrak{p})$ è l'insieme degli elementi ≥ 0 in un sottogruppo isolato Δ di Γ, e che l'applicazione così definita di Spec(A) nell'insieme dei sottogruppi isolati di Γ è biiettiva.

    Se $\mathfrak{p}$ è un ideale primo di A, quali sono i gruppi dei valori degli anelli di valutazione $A/\mathfrak{p}$, $A_\mathfrak{p}$?

33. Sia Γ un gruppo abeliano totalmente ordinato. Mostreremo come costruire un campo K e una valutazione v di K avente Γ come gruppo dei valori. Sia k un campo arbitrario e sia $A = k[\Gamma]$ l'algebra-gruppo di Γ su k. Per definizione, A è generato liberamente, come k-spazio vettoriale, da elementi $x_\alpha (\alpha \in \Gamma)$ tali che $x_\alpha x_\beta = x_{\alpha+\beta}$. Provare che A è un dominio di integrità.

    Se $u = \lambda_1 x_{\alpha_1} + \ldots + \lambda_n x_{\alpha_n}$ è un arbitrario elemento non nullo di A, dove i λ_i sono tutti $\neq 0$ e $\alpha_1 < \quad < \alpha_n$, definiamo $v_0(u) = \alpha_1$. Provare che l'applicazione $v_0: A - \{0\} \to \Gamma$ soddisfa le condizioni (1) e (2) dell'Esercizio 31.

    Sia K il campo delle frazioni di A. Dimostrare che l'applicazione v_0 può essere estesa in modo unico ad una valutazione v di K, e che il gruppo dei valori di v è precisamente Γ.

34. Sia A un anello di valutazione e K il suo campo delle frazioni. Sia $f: A \to B$ un omomorfismo di anelli tale che f^*: Spec$(B) \to$ Spec(A) è un'applicazione *chiusa*. Allora, se $g: B \to K$ è un arbitrario omomorfismo di A-algebre (ossia, se $g \circ f$ è l'immersione di A in K), si ha $g(B) = A$.

[Poniamo $C = g(B)$; ovviamente $C \supseteq A$. Sia $\mathfrak{n}$ un ideale massimale di C. Poiché f^* è chiusa, $\mathfrak{m} = \mathfrak{n} \cap A$ è l'ideale massimale di A, sicché $A_\mathfrak{m} = A$. Inoltre l'anello locale $C_\mathfrak{n}$ domina $A_\mathfrak{m}$. Dunque, in virtú dell'Esercizio 27, si ha $C_\mathfrak{n} = A$, e pertanto $C \subseteq A$.]

35. Dagli Esercizi 1 e 3 segue che, se $f\colon A \to B$ è un omomorfismo intero e C è una A-algebra arbitraria, allora l'applicazione $(f \otimes 1)^*$ $\operatorname{Spec}(B \otimes_A C) \to \operatorname{Spec}(C)$ è chiusa.

Viceversa, supponiamo che $f\colon A \to B$ abbia tale proprietà e che B sia un dominio di integrità. Allora f è intero. [Sostituendo A con la sua immagine in B, ci riduciamo al caso in cui $A \subseteq B$ e f è l'identità. Sia K il campo delle frazioni di B e sia A' un anello di valutazione di K contenente A. In virtú di (5.22), basta provare che A' contiene B. Per ipotesi $\operatorname{Spec}(B \otimes_A A') \to \operatorname{Spec}(A')$ è un'applicazione chiusa. Applichiamo il risultato dell'Esercizio 34 all'omomorfismo $B \otimes_A A' \to K$ definito da $b \otimes a' \mapsto ba'$. Ne segue che $ba' \in A'$ per ogni $b \in B$ e per ogni $a' \in A'$; prendendo $a' = 1$, si ottiene la tesi.]

Dimostrare che il risultato ora provato resta valido se B è un anello che possiede soltanto un numero finito di ideali primi minimali (per es., se B è noetheriano). [Siano $\mathfrak{p}_i$ gli ideali primi minimali. Allora ciascun omomorfismo composto $A \to B \to B/\mathfrak{p}_i$ è intero, sicché $A \to \Pi\,(B/\mathfrak{p}_i)$ è intero, dunque $A \to B/\mathfrak{N}$ è intero (dove $\mathfrak{N}$ è il nilradicale di B), e finalmente $A \to B$ è intero.]

Il risultato in questione continua a valere in generale, senza ipotesi restrittive su B?

Capitolo sesto

Condizioni sulle catene

Fino ad ora abbiamo considerato anelli commutativi (con unità) del tutto arbitrari. Tuttavia, per procedere oltre e ottenere risultati piú profondi, è necessario imporre alcune condizioni di finitezza. Il modo piú conveniente è quello delle "condizioni sulle catene". Esse si applicano sia agli anelli che ai moduli, e in questo capitolo consideriamo il caso dei moduli. La maggior parte delle argomentazioni hanno un carattere piuttosto formale, e a causa di ciò, vi è una simmetria tra le catene ascendenti e le catene discendenti—una simmetria che scompare nel caso degli anelli, come vedremo nei capitoli successivi.

Sia Σ un insieme parzialmente ordinato mediante una relazione $\leqslant$ (ossia, $\leqslant$ è riflessiva e transitiva ed è tale che $x \leqslant y$ e $y \leqslant x$ insieme implicano $x = y$).

Proposizione 6.1. *Le seguenti condizioni su Σ sono equivalenti:*

i) *Ogni successione crescente $x_1 \leqslant x_2 \leqslant$ in Σ è stazionaria* (*ossia, esiste un intero n tale che $x_n = x_{n+1} = \ldots$*).

ii) *Ogni sottoinsieme non vuoto di Σ possiede un elemento massimale.*

Dimostrazione. i) $\Rightarrow$ ii). Supponiamo che ii) non sia vera; allora esiste un sottoinsieme non vuoto T di Σ privo di elementi massimali, e si può costruire induttivamente una successione strettamente crescente non stazionaria in T.

ii) $\Rightarrow$ i). L'insieme $(x_m)_{m \geqslant 1}$ possiede un elemento massimale, diciamo x_n. ■

Se Σ è l'insieme dei sottomoduli di un modulo M, ordinato mediante la relazione $\subseteq$, allora la i) prende il nome di *condizione della catena ascendente* (a.c.c. in breve) e la ii) prende il nome di *condizione massimale*. Un modulo M che soddisfa l'una o l'altra di tali condizioni equivalenti si dice *noetheriano* (in onore di Emmy Noether). Se Σ è ordinato mediante la relazione $\supseteq$, allora la i) è la *condizione della catena discendente* (d.c.c. in breve) e la ii) è la *condizione minimale*. Un modulo M che soddisfa ad esse si dice *artiniano* (in onore di Emil Artin).

Esempi. 1) Un gruppo abeliano finito (come $\mathbf{Z}$-modulo) soddisfa sia la a.c.c. che la d.c.c.

2) L'anello $\mathbf{Z}$ (come $\mathbf{Z}$-modulo) soddisfa la a.c.c. ma non la d.c.c. Infatti, se $a \in \mathbf{Z}$ e $a \neq 0, \pm 1$, si ha $(a) \supset (a^2) \supset \quad \supset (a^n) \supset$ (inclusioni strette).

3) Sia G il sottogruppo di $\mathbf{Q}/\mathbf{Z}$ formato da tutti gli elementi il cui ordine è una potenza di p, dove p è un numero primo fissato. Allora G possiede esattamente un unico sottogruppo G_n di ordine p^n per ogni $n \geqslant 0$, e si ha $G_0 \subset G_1 \subset \ldots \subset G_n \subset \ldots$ (inclusioni strette), sicché G non soddisfa la a.c.c. D'altra parte gli unici sottogruppi propri di G sono i G_n, dunque G soddisfa la d.c.c.

4) Il gruppo H di tutti i numeri razionali della forma m/p^n (m, $n \in \mathbf{Z}$, $n \geqslant 0$) non soddisfa alcuna condizione sulle catene. Infatti si ha una successione esatta $0 \to \mathbf{Z} \to H \to G \to 0$, sicché H non soddisfa la d.c.c. poiché $\mathbf{Z}$ non la soddisfa, e H non soddisfa la a.c.c. poiché G non la soddisfa.

5) L'anello $k[x]$ (dove k è un campo e x è un'indeterminata) soddisfa la a.c.c. ma non la d.c.c. sugli *ideali*.

6) L'anello dei polinomi $k[x_1, x_2, \ldots]$ in un numero infinito di indeterminate x_n non soddisfa *alcuna* condizione sulle catene di ideali: infatti la successione $(x_1) \subset (x_1, x_2) \subset \ldots$ è strettamente crescente, e la successione $(x_1) \supset (x_1^2) \supset (x_1^3) \supset$ è strettamente decrescente.

7) Vedremo più avanti che un anello che soddisfa la d.c.c. sugli ideali deve soddisfare anche la a.c.c. sugli ideali. (Ciò *non* è vero per i moduli, in generale: cfr. gli esempi precedenti 2) e 3)).

Proposizione 6.2. *M è un A-modulo noetheriano $\Leftrightarrow$ ogni sottomodulo di M è finitamente generato.*

Dimostrazione. $\Rightarrow$: Sia N un sottomodulo di M, e sia Σ l'insieme di tutti i sottomoduli finitamente generati di N. Allora Σ è non vuoto (giacché $0 \in \Sigma$) e pertanto possiede un elemento massimale, diciamo N_0. Se $N_0 \neq N$, consideriamo il sottomodulo $N_0 + Ax$, dove $x \in N$, $x \notin N_0$; esso è finitamente generato e contiene strettamente N_0, sicché si ottiene una contraddizione. Ne segue che $N = N_0$ e pertanto N è finitamente generato.

$\Leftarrow$: Sia $M_1 \subseteq M_2 \subseteq$ una catena ascendente di sottomoduli di M. Allora $N = \bigcup_{n=1}^{\infty} M_n$ è un sottomodulo di M, dunque è generato da un numero finito di elementi, diciamo $x_1, \ldots, x_r$. Supponiamo che $x_i \in M_{n_i}$ e poniamo $n = \max_{1 \leq i \leq r} n_i$; allora ciascun $x_i \in M_n$, dunque $M_n = M$ e pertanto la catena è stazionaria. ∎

In virtú di (6.2), i moduli noetheriani sono piú importanti dei moduli artiniani: la noetherianità è proprio la condizione di finitezza che serve per la validità di una quantità notevole di teoremi. Tuttavia, molte proprietà formali elementari valgono sia per i moduli noetheriani che per i moduli artiniani.

Proposizione 6.3. *Sia* $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ *una successione esatta di* A*-moduli. Allora*:

i) M *è noetheriano* $\Leftrightarrow$ M' *e* M'' *sono noetheriani*;

ii) M *è artiniano* $\Leftrightarrow$ M' *e* M'' *sono artiniani.*

Dimostrazione. Proveremo solo i); ii) si dimostra in modo simile.

$\Rightarrow$: Una catena ascendente di sottomoduli di M' (o di M'') dà origine ad una catena in M, dunque è stazionaria.

$\Leftarrow$: Sia $(L_n)_{n \geq 1}$ una catena ascendente di sottomoduli di M; allora $(\alpha^{-1}(L_n))$ è una catena in M', e $(\beta(L_n))$ è una catena in M''. Per n abbastanza grande tali catene sono entrambe stazionarie, da cui segue che la catena (L_n) è stazionaria. ∎

Corollario 6.4. *Se* M_i $(1 \leq i \leq n)$ *sono* A*-moduli noetheriani* (*risp. artiniani*), *tale risulta* $\bigoplus_{i=1}^{n} M_i$.

Dimostrazione. Si procede per induzione, applicando (6.3) alla successione esatta

$$0 \to M_n \to \bigoplus_{i=1}^{n} M_i \to \bigoplus_{i=1}^{n-1} M_i \to 0. \quad ∎$$

Un anello A si dice *noetheriano* (risp. *artiniano*) se risulta tale come A-modulo, ossia, se soddisfa la a.c.c. (risp. la d.c.c.) sugli ideali.

Esempi. 1) Ogni campo è artiniano e noetheriano; tale è anche l'anello $\mathbf{Z}/(n)$ $(n \neq 0)$. L'anello $\mathbf{Z}$ è noetheriano, ma non artiniano (cfr. l'esempio 2 prima di (6.2)).

2) Ogni dominio a ideali principali è noetheriano (in virtú di (6.2): ogni ideale è finitamente generato).

3) L'anello $k[x_1, x_2, \ldots]$ non è noetheriano (cfr. l'esempio 6 precedente). Tuttavia esso è un dominio di integrità, dunque possiede un campo di frazioni. Cosí un *subanello* di un anello noetheriano non è necessariamente noetheriano.

4) Sia X uno spazio compatto di Hausdorff infinito, $C(X)$ l'anello delle funzioni a valori reali continue su X. Prendiamo una successione strettamente decrescente $F_1 \supset F_2 \supset \cdots$ di chiusi in X e poniamo $\mathfrak{a}_n = \{f \in C(X) : f(F_n) = 0\}$. Allora gli $\mathfrak{a}_n$ formano una successione strettamente crescente di ideali in $C(X)$: dunque $C(X)$ non è un anello noetheriano.

Proposizione 6.5. *Sia A un anello noetheriano (risp. artiniano), M un A-modulo finitamente generato. Allora M è noetheriano (risp. artiniano).*

Dimostrazione. M è un quoziente di A^n per qualche n: applicare (6.4) e (6.3). ∎

Proposizione 6.6. *Sia A un anello noetheriano (risp. artiniano), $\mathfrak{a}$ un ideale di A. Allora $A/\mathfrak{a}$ è un anello noetheriano (risp. artiniano).*

Dimostrazione. In virtú di (6.3), $A/\mathfrak{a}$ è noetheriano (risp. artiniano) come A-modulo, dunque anche come $A/\mathfrak{a}$-modulo. ∎

Una *catena* di sottomoduli di un modulo M è una successione (M_i) $(0 \leqslant i \leqslant n)$ di sottomoduli di M tali che

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0 \text{ (inclusioni } \textit{strette}\text{).}$$

La *lunghezza* della catena è n (il numero dei "legami"). Una *serie di composizione* di M è una catena massimale, cioè una catena in cui non è possibile inserire ulteriori sottomoduli: ciò equivale a dire che ciascun quoziente M_{i-1}/M_i $(1 \leqslant i \leqslant n)$ è *semplice* (ossia, non possiede altri sottomoduli al di fuori di 0 e se stesso).

Proposizione 6.7. *Supponiamo che M abbia una serie di composizione di lunghezza n. Allora ogni serie di composizione di M ha lunghezza n, e ogni catena in M può essere estesa ad una serie di composizione.*

Dimostrazione. Denotiamo con $l(M)$ la lunghezza minima di una serie di composizione di un modulo M. ($l(M) = +\infty$ se M non possiede serie di composizione.)

i) $N \subset M \Rightarrow l(N) < l(M)$. Sia (M_i) una serie di composizione di M di lunghezza minima, e consideriamo i sottomoduli $N_i = N \cap M_i$ di N. Poiché $N_{i-1}/N_i \subseteq M_{i-1}/M_i$ e il secondo è un modulo semplice, si ha: $N_{i-1}/N_i = M_{i-1}/M_i$, oppure $N_{i-1} = N_i$; dunque, eliminando termini ripetuti, si ottiene una serie di composizione di N, sicché $l(N) \leqslant l(M)$. Se $l(N) = l(M) = n$, allora $N_{i-1}/N_i = M_{i-1}/M_i$ per ciascun indice $i = 1, 2, \ldots, n$; ne segue che $M_{n-1} = N_{n-1}$, da cui $M_{n-2} = N_{n-2}, \ldots$, e finalmente $M = N$.

ii) *Ogni catena in M ha lunghezza $\leqslant l(M)$.* Sia $M = M_0 \supset M_1 \supset \ldots$ una catena di lunghezza k. Allora, in virtú di i), si ha $l(M) > l(M_1) > \ldots > l(M_k) = 0$, da cui $l(M) \geqslant k$.

iii) Consideriamo un'arbitraria serie di composizione di M. Se essa ha lunghezza k, allora $k \leqslant l(M)$, in virtú di ii), sicché $k = l(M)$ per definizione di $l(M)$. Dunque tutte le serie di composizione hanno la stessa lunghezza. Infine, consideriamo una catena qualsiasi. Se la sua lunghezza è $l(M)$, essa deve essere una serie di composizione, stante ii); se la sua lunghezza è $< l(M)$, essa non è una serie di composizione, dunque non è massimale e pertanto è possibile inserire nuovi termini fino a che la lunghezza è $l(M)$. ■

Proposizione 6.8. *M possiede una serie di composizione $\Leftrightarrow$ M soddisfa entrambe le condizioni sulle catene.*

Dimostrazione. $\Rightarrow$: Tutte le catene in M hanno lunghezza limitata, dunque valgono sia la a.c.c. che la d.c.c.

$\Leftarrow$: Costruiamo una serie di composizione di M nel modo seguente. Poiché $M = M_0$ soddisfa la condizione massimale, in virtú di (6.1), esso possiede un sottomodulo massimale $M_1 \subset M_0$. Similmente M_1 possiede un sottomodulo massimale $M_2 \subset M_1$, e cosí via. Si ottiene cosí una catena strettamente decrescente $M_0 \supset M_1 \supset \ldots$ la quale deve risultare finita, in virtú della d.c.c., e quindi è una serie di composizione di M. ■

Un modulo che soddisfa sia la a.c.c. che la d.c.c. è chiamato pertanto un *modulo di lunghezza finita*. In virtú di (6.7) tutte le serie di composizione di M hanno la medesima lunghezza $l(M)$, che prende il nome di *lunghezza di M*. Il teorema di Jordan-Hölder si applica ai moduli di lunghezza finita: se $(M_i)_{0 \leqslant i \leqslant n}$ e $(M'_i)_{0 \leqslant i \leqslant n}$ sono due serie di composizione arbitrarie di M, vi è una corrispondenza biunivoca tra l'insieme dei quozienti $(M_{i-1}/M_i)_{1 \leqslant i \leqslant n}$ e l'insieme dei quozienti $(M'_{i-1}/M'_i)_{1 \leqslant i \leqslant n}$, tale che quozienti corrispondenti sono isomorfi. La dimostrazione è la stessa di quella per i gruppi finiti.

Proposizione 6.9. *La lunghezza $l(M)$ è una funzione additiva sulla classe di tutti gli A-moduli di lunghezza finita.*

Dimostrazione. Occorre provare che, se $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ è una successione esatta, allora $l(M) = l(M') + l(M'')$. Consideriamo l'immagine rispetto a α di una arbitraria serie di composizione di M' e la controimmagine rispetto a β di una arbitraria serie di composizione di M''; esse si raccordano dando origine ad una serie di composizione di M, donde la tesi. ∎

Consideriamo il caso particolare dei moduli sopra un campo k, ossia, dei k-spazi vettoriali:

Proposizione 6.10. *Per un k-spazio vettoriale V le seguenti condizioni sono equivalenti:*

i) *dimensione finita;*
ii) *lunghezza finita;*
iii) *a.c.c.;*
iv) *d.c.c.*

Inoltre, se tali condizioni sono soddisfatte, la lunghezza risulta uguale alla dimensione.

Dimostrazione. i) $\Rightarrow$ ii) è banale; ii) $\Rightarrow$ iii) e ii) $\Rightarrow$ iv) discendono da (6.8). Resta da provare che iii) $\Rightarrow$ i) e iv) $\Rightarrow$ i). Supponiamo che la i) non sia vera, allora esiste una successione infinita $(x_n)_{n \geq 1}$ di elementi di V linearmente indipendenti. Sia U_n (risp. V_n) lo spazio vettoriale generato da $x_1, \ldots, x_n$ (risp. $x_{n+1}, x_{n+2}, \ldots$). Allora la successione $(U_n)_{n \geq 1}$ (risp. $(V_n)_{n \geq 1}$) è infinita e strettamente crescente (risp. strettamente decrescente). ∎

Corollario 6.11. *Sia A un anello in cui l'ideale zero è un prodotto $\mathfrak{m}_1 \cdots \mathfrak{m}_n$ di ideali massimali (non necessariamente distinti). Allora A è noetheriano se e soltanto se A è artiniano.*

Dimostrazione. Consideriamo la catena di ideali $A \supset \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq$ $\supseteq \mathfrak{m}_1 \quad \mathfrak{m}_n = 0$. Ciascun quoziente $\mathfrak{m}_1 \quad \mathfrak{m}_{i-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i$ è uno spazio vettoriale sul campo $A/\mathfrak{m}_i$. Dunque a.c.c. $\Leftrightarrow$ d.c.c. per ciascun quoziente. Ma a.c.c. (risp. d.c.c.) per ciascun quoziente $\Leftrightarrow$ a.c.c. (risp. d.c.c.) per A, com'è subito visto applicando (6.3). Dunque a.c.c. $\Leftrightarrow$ d.c.c. per A. ∎

Esercizi

1. i) Sia M un A-modulo noetheriano e $u: M \to M$ un omomorfismo di moduli. Se u è suriettivo, allora u è un isomorfismo.

   ii) Se M è artiniano e u è iniettivo, allora u è un isomorfismo.

   [Per provare (i), considerare i sottomoduli $\operatorname{Ker}(u^n)$; per (ii), i moduli quozienti $\operatorname{Coker}(u^n)$.]

2. Sia M un A-modulo. Se ogni insieme non vuoto di sottomoduli finitamente generati di M possiede un elemento massimale, allora M è noetheriano.

3. Sia M un A-modulo e siano N_1, N_2 sottomoduli di M. Se M/N_1 e M/N_2 sono noetheriani, tale risulta $M/(N_1 \cap N_2)$. Un risùltato simile vale sostituendo "noetheriano" con "artiniano".

4. Sia M un A-modulo noetheriano e sia $\mathfrak{a}$ l'annullatore di M in A. Dimostrare che $A/\mathfrak{a}$ è un anello noetheriano.

   Se si sostituisce "noetheriano" con "attiniano", il risultato è ancora vero?

5. Uno spazio topologico X si dice *noetheriano* se gli aperti di X soddisfano la condizione della catena ascendente (o, in modo equivalente, la condizione massimale). Poiché i chiusi sono i complementari degli aperti, ciò equivale a dire che i chiusi di X soddisfano la condizione della catena discendente (o, in modo equivalente, la condizione minimale). Provare che, se X è noetheriano, allora ogni sottospazio di X è noetheriano, e inoltre che X è quasi-compatto.

6. Dimostrare che le seguenti condizioni sono equivalenti per uno spazio topologico X:

   i) X è noetheriano.

   ii) Ogni aperto di X è quasi-compatto.

   iii) Ogni sottospazio di X è quasi-compatto.

7. Uno spazio noetheriano è un'unione finita di sottospazi chiusi irriducibili. [Considerare l'insieme Σ dei chiusi di X che non sono unioni finite di chiusi irriducibili.] Dunque l'insieme delle componenti irriducibili di uno spazio noetheriano è finito.

8. Se A è un anello noetheriano, allora $\operatorname{Spec}(A)$ è uno spazio topologico noetheriano. Vale il viceversa?

9. Dedurre dall'Esercizio 7 che l'insieme degli ideali primi minimali in un anello noetheriano è finito.

10. Se M è un modulo noetheriano (su un anello arbitrario A), allora Supp (M) è un sottospazio noetheriano chiuso di Spec (A).

11. Sia $f: A \to B$ un omomorfismo di anelli e supponiamo che Spec (B) sia uno spazio noetheriano (Esercizio 5). Provare che f^*: Spec $(B) \to$ Spec (A) è un'applicazione chiusa se e soltanto se f possiede la proprietà del going-up (Capitolo 5, Esercizio 10). Tale risultato continua a valere in generale, senza ipotesi restrittive su Spec (B)?

12. Sia A un anello tale che Spec (A) è uno spazio noetheriano. Dimostrare che l'insieme degli ideali primi di A soddisfa la condizione della catena ascendente. Vale il viceversa?

Capitolo settimo

Anelli noetheriani

Ricordiamo che un anello A si dice *noetheriano* se soddisfa una delle tre seguenti condizioni, tra loro equivalenti:

1) Ogni insieme non vuoto di ideali in A possiede un elemento massimale.

2) Ogni catena ascendente di ideali in A è stazionaria.

3) Ogni ideale di A è finitamente generato.

(L'equivalenza di tali condizioni è stata provata in (6.1) e (6.2).)

Gli anelli noetheriani costituiscono senz'altro la classe piú importante di anelli in algebra commutativa: abbiamo già visto alcuni esempi nel Capitolo 6. In questo capitolo mostreremo dapprima che gli anelli noetheriani sono stabili rispetto a varie operazioni ben note: in particolare, dimostriamo il celebre teorema della base di Hilbert. Successivamente, dedurremo alcune importanti conseguenze dalla noetherianità, compresa l'esistenza delle decomposizioni primarie.

Proposizione 7.1. *Se A è noetheriano e ϕ è un omomorfismo di A su un anello B, allora B è noetheriano.*

Dimostrazione. Ciò segue da (6.6), poiché $B \cong A/\mathfrak{a}$, dove $\mathfrak{a} = \operatorname{Ker}(\phi)$. ∎

Proposizione 7.2. *Sia A un subanello di B; supponiamo che A sia noetheriano e che B sia finitamente generato come A-modulo. Allora B è noetheriano (come anello).*

Dimostrazione. In virtú di (6.5) B è noetheriano come A-modulo, dunque anche come B-modulo. ∎

Esempio. $B = \mathbf{Z}[i]$, l'anello degli interi di Gauss. In virtú di (7.2) B è noetheriano. Piú in generale, l'anello degli interi in un arbitrario campo di numeri algebrici è noetheriano.

Proposizione 7.3. *Se A è noetheriano e S è una parte moltiplicativa arbitraria di A, allora $S^{-1}A$ è noetheriano.*

Dimostrazione. In virtú di (3.11—i)) e (1.17—iii)), vi è una corrispondenza biunivoca, che conserva l'ordinamento, tra gli ideali di $S^{-1}A$ e gli ideali contratti di A, dunque gli ideali di $S^{-1}A$ soddisfano la condizione massimale. (Dimostrazione alternativa: se $\mathfrak{a}$ è un ideale qualsiasi di A, allora $\mathfrak{a}$ possiede un sistema finito di generatori, diciamo $x_1, \ldots, x_n$, ed è chiaro che $S^{-1}\mathfrak{a}$ è generato da $x_1/1, \ldots, x_n/1$.) ■

Corollario 7.4. *Se A è noetheriano e $\mathfrak{p}$ è un ideale primo di A, allora $A_\mathfrak{p}$ è noetheriano.* ■

Teorema 7.5. (Teorema della base di Hilbert). *Se A è noetheriano, allora l'anello dei polinomi $A[x]$ è noetheriano.*

Dimostrazione. Sia $\mathfrak{a}$ un ideale di $A[x]$. I coefficienti direttori dei polinomi in $\mathfrak{a}$ formano un ideale $\mathfrak{l}$ in A. Poiché A è noetheriano, $\mathfrak{l}$ è finitamente generato, diciamo da $a_1, \ldots, a_n$. Per ciascun indice $i = 1, \ldots, n$ esiste un polinomio $f_i \in \mathfrak{a}$ della forma $f_i = a_i x^{r_i} +$ (termini di grado piú basso). Poniamo $r = \max_{1 \leq i \leq n} r_i$. Gli f_i generano un ideale $\mathfrak{a}' \subseteq \mathfrak{a}$ in $A[x]$.

Sia $f = ax^m +$ (termini di grado piú basso) un elemento arbitrario di $\mathfrak{a}$; si ha: $a \in \mathfrak{l}$. Se $m \geq r$, scriviamo $a = \sum_{i=1}^{n} u_i a_i$, dove $u_i \in A$; allora il polinomio $f - \sum u_i f_i x^{m-r_i}$ appartiene ad $\mathfrak{a}$ e ha grado $< m$. Procedendo in tal modo, possiamo sottrarre da f elementi di $\mathfrak{a}'$ fino ad ottenere un polinomio g, diciamo, di grado $< r$; ossia, si ha: $f = g + h$, con $h \in \mathfrak{a}'$.

Sia M l'A-modulo generato da $1, x, \ldots, x^{r-1}$; allora ciò che abbiamo provato è che $\mathfrak{a} = (\mathfrak{a} \cap M) + \mathfrak{a}'$. Ora M è un A-modulo finitamente generato, dunque è noetheriano in virtú di (6.5), e quindi $\mathfrak{a} \cap M$ è finitamente generato (come A-modulo) in virtú di (6.2). Se $g_1, \ldots, g_m$ generano $\mathfrak{a} \cap M$, è chiaro che gli f_i e i g_j generano $\mathfrak{a}$. Dunque $\mathfrak{a}$ è finitamente generato e quindi $A[x]$ è noetheriano. ■

Osservazione. È vero inoltre che A noetheriano $\Rightarrow A[[x]]$ noetheriano (essendo $A[[x]]$ l'anello delle serie di potenze formali in x a coefficienti in A). La dimostrazione procede quasi parallelamente a quella di (7.5), eccettuato il fatto che si parte dai termini di grado *minimo* nelle serie di potenze appartenenti ad $\mathfrak{a}$. Cfr. anche (10.27).

Corollario 7.6. *Se A è noetheriano, tale risulta l'anello $A[x_1, \dots, x_n]$.*

Dimostrazione. Si procede per induzione su n, partendo da (7.5). ■

Corollario 7.7. *Sia B una A-algebra finitamente generata. Se A è noetheriano, tale risulta B.*

In particolare, ogni anello finitamente generato, e ogni algebra finitamente generata sopra un campo, è un anello noetheriano.

Dimostrazione. B è un'immagine omomorfa di un anello di polinomi $A[x_1, \dots, x_n]$, il quale è noetheriano in virtú di (7.6). ■

Proposizione 7.8. *Siano $A \subseteq B \subseteq C$ anelli. Supponiamo che A sia noetheriano, C sia una A-algebra finitamente generata, e supponiamo inoltre che C sia* (i) *finitamente generato come B-modulo oppure* (ii) *intero su B. Allora B è una A-algebra finitamente generata.*

Dimostrazione. Da (5.1) e (5.2) segue che le condizioni (i) e (*ii*) sono equivalenti, nelle nostre ipotesi. Dunque possiamo limitarci a considerare la condizione (i).

Siano $x_1, \dots, x_m$ un sistema di generatori di C come A-algebra, e $y_1, \dots, y_n$ un sistema di generatori di C come B-modulo. Allora esistono espressioni della forma:

$$x_i = \sum_j b_{ij} y_j \qquad (b_{ij} \in B) \tag{1}$$

$$y_i y_j = \sum_k b_{ijk} y_k \qquad (b_{ijk} \in B). \tag{2}$$

Sia B_0 la A-algebra generata dagli elementi b_{ij} e b_{ijk}. Poiché A è noetheriano, tale risulta B_0 in virtú di (7.7), e $A \subseteq B_0 \subseteq B$.

Un elemento arbitrario di C è un polinomio negli x_i a coefficienti in A. Sostituendo le (1) e facendo un uso ripetuto delle (2) si ha che ogni elemento di C risulta una combinazione lineare degli y_j a coefficienti in B_0, e dunque C è finitamente generato come B_0-modulo. Poiché B_0 è noetheriano, e B è un sottomodulo di C, segue (da (6.5) e (6.2)) che B è finitamente generato come B_0-modulo. Ma B_0 è una A-algebra finitamente generata, dunque B è una A-algebra finitamente generata. ■

Proposizione 7.9. *Sia k un campo, E una k-algebra finitamente generata. Se E è un campo, allora E è un'estensione algebrica finita di k.*

Dimostrazione. Sia $E = k[x_1, \dots, x_n]$. Se E non è un'estensione algebrica di k, allora possiamo rinumerare gli x_i in modo tale che $x_1, \dots, x_r$ siano algebricamente indipendenti su k, dove $r \geqslant 1$, e ciascuno degli elementi $x_{r+1}, \ldots, x_n$ è algebrico sul campo $F = k(x_1, \ldots, x_r)$. Dunque E è un'estensione algebrica finita di F e pertanto è finitamente generato come F-modulo. Applicando (7.8) a $k \subseteq F \subseteq E$, si ha che F è una k-algebra finitamente generata, diciamo $F = k[y_1, \ldots, y_s]$. Ciascun y_j è della forma f_j/g_j, dove f_j e g_j sono polinomi in $x_1, \ldots, x_r$.

Ora nell'anello $k[x_1, \ldots, x_r]$ vi sono infiniti polinomi irriducibili (basta adattare la dimostrazione di Euclide dell'esistenza di infiniti numeri primi). Ne segue che esiste un polinomio irriducibile h, il quale risulta primo rispetto a ciascuno dei polinomi g_j (basta prendere un fattore irriducibile del polinomio $g_1 g_2 \cdots g_s + 1$) e allora l'elemento h^{-1} di F non potrebbe essere espresso come un polinomio negli y_j. Ciò è una contraddizione. Dunque E è un'estensione algebrica di k, e pertanto algebrica finita. ∎

Corollario 7.10. *Sia k un campo, A una k-algebra finitamente generata. Sia $\mathfrak{m}$ un ideale massimale di A. Allora il campo $A/\mathfrak{m}$ è un'estensione algebrica finita di k. In particolare, se k è algebricamente chiuso, allora $A/\mathfrak{m} \cong k$.*

Dimostrazione. Basta prendere $E = A/\mathfrak{m}$ in (7.9). ∎

L'enunciato (7.10) è la cosiddetta forma "debole" del teorema degli zeri di Hilbert. La dimostrazione data qui è dovuta ad Artin e Tate. Per il suo significato geometrico, e per la forma "forte" del teorema, consultare gli esercizi alla fine del capitolo.

Decomposizione primaria negli anelli noetheriani

I due lemmi seguenti mostrano che ogni ideale $\neq (1)$ in un anello noetheriano possiede una decomposizione primaria.

Un ideale $\mathfrak{a}$ si dice *irriducibile* se

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Rightarrow (\mathfrak{a} = \mathfrak{b} \text{ oppure } \mathfrak{a} = \mathfrak{c}).$$

Lemma 7.11. *In un anello noetheriano A ogni ideale è un'intersezione finita di ideali irriducibili.*

Dimostrazione. Supponiamo che la tesi non sia vera; allora l'insieme degli ideali di A per i quali il lemma è falso è non vuoto, dunque possiede un elemento massimale $\mathfrak{a}$. Poiché $\mathfrak{a}$ è riducibile, si ha: $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$, dove $\mathfrak{b} \supset \mathfrak{a}$ e $\mathfrak{c} \supset \mathfrak{a}$. Dunque ciascuno degli ideali $\mathfrak{b}, \mathfrak{c}$ è un'intersezione finita di ideali irriducibili e pertanto tale risulta $\mathfrak{a}$, ciò che è una contraddizione. ∎

Lemma 7.12. *In un anello noetheriano ogni ideale irriducibile è primario.*

Dimostrazione. Passando all'anello quoziente, è sufficiente far vedere che se l'ideale zero è irriducibile, allora è primario. Sia $xy = 0$ con $y \neq 0$, e consideriamo la catena di ideali $\operatorname{Ann}(x) \subseteq \operatorname{Ann}(x^2) \subseteq \dots$. In virtú della a.c.c., tale catena è stazionaria, ossia si ha $\operatorname{Ann}(x^n) = \operatorname{Ann}(x^{n+1}) = \dots$ per qualche n. Ne segue che $(x^n) \cap (y) = 0$; infatti, se $a \in (y)$ allora $ax = 0$, e se $a \in (x^n)$ allora $a = bx^n$, sicché $bx^{n+1} = 0$, da cui $b \in \operatorname{Ann}(x^{n+1}) = \operatorname{Ann}(x^n)$, e quindi $bx^n = 0$, ossia $a = 0$. Poiché (0) è irriducibile e $(y) \neq 0$ si ottiene necessariamente $x^n = 0$, e ciò prova che (0) è primario. ∎

Dai due lemmi precedenti si ottiene subito il

Teorema 7.13. *In un anello neotheriano A ogni ideale possiede una decomposizione primaria.* ∎

Dunque tutti i risultati del Capitolo 4 si applicano agli anelli noetheriani.

Proposizione 7.14. *In un anello noetheriano A, ogni ideale $\mathfrak{a}$ contiene una potenza del proprio radicale.*

Dimostrazione. Siano $x_1, \dots, x_k$ un sistema di generatori di $r(\mathfrak{a})$: diciamo $x_i^{n_i} \in \mathfrak{a}$ $(1 \leqslant i \leqslant k)$. Poniamo $m = \sum_{i=1}^{k} (n_i - 1) + 1$. Allora $r(\mathfrak{a})^m$ è generato dai prodotti $x_1^{r_1} \dots x_k^{r_k}$ con $\sum r_i = m$; dalla definizione di m si ha necessariamente $r_i \geqslant n_i$ per almeno un indice i, sicché ciascuno di tali monomi appartiene ad $\mathfrak{a}$, e pertanto $r(\mathfrak{a})^m \subseteq \mathfrak{a}$. ∎

Corollario 7.15. *In un anello noetheriano il nilradicale è nilpotente.*

Dimostrazione. Basta prendere $\mathfrak{a} = (0)$ in (7.14). ∎

Corollario 7.16. *Sia A un anello noetheriano, $\mathfrak{m}$ un ideale massimale di A, $\mathfrak{q}$ un ideale arbitrario di A. Allora le seguenti condizioni sono equivalenti*:

i) $\mathfrak{q}$ *è* $\mathfrak{m}$-*primario*;
ii) $r(\mathfrak{q}) = \mathfrak{m}$;
iii) $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ *per qualche* $n > 0$.

Dimostrazione. i) $\Rightarrow$ ii) è banale. ii) $\Rightarrow$ i) segue da (4.2), ii) $\Rightarrow$ iii) segue da (7.14); iii) $\Rightarrow$ ii) si ottiene prendendo i radicali: $\mathfrak{m} = r(\mathfrak{m}^n) \subseteq r(\mathfrak{q}) \subseteq r(\mathfrak{m}) = \mathfrak{m}$. ∎

Proposizione 7.17. *Sia* $\mathfrak{a} \neq (1)$ *un ideale in un anello noetheriano. Allora gli ideali primi che appartengono ad* $\mathfrak{a}$ *sono precisamente gli ideali primi che compaiono nell'insieme degli ideali* $(\mathfrak{a}:x)$ $(x \in A)$.

Dimostrazione. Passando ad $A/\mathfrak{a}$ possiamo supporre che $\mathfrak{a} = 0$. Sia $\bigcap_{i=1}^{n} \mathfrak{q}_i = 0$ una decomposizione primaria minimale dell'ideale zero, e sia $\mathfrak{p}_i$ il radicale di $\mathfrak{q}_i$. Poniamo $\mathfrak{a}_i = \bigcap_{j \neq i} \mathfrak{q}_j \neq 0$. Allora, dalla dimostrazione di (4.5) si ha $r(\mathrm{Ann}\,(x)) = \mathfrak{p}_i$, per un arbitrario elemento $x \neq 0$ in $\mathfrak{a}_i$, sicché $\mathrm{Ann}\,(x) \subseteq \mathfrak{p}_i$.

Poiché $\mathfrak{q}_i$ è $\mathfrak{p}_i$-primario, in virtú di (7.14) esiste un intero m tale che $\mathfrak{p}_i^m \subseteq \mathfrak{q}_i$, e pertanto $\mathfrak{a}_i\mathfrak{p}_i^m \subseteq \mathfrak{a}_i \cap \mathfrak{p}_i^m \subseteq \mathfrak{a}_i \cap \mathfrak{q}_i = 0$. Sia $m \geqslant 1$ il piú piccolo intero tale che $\mathfrak{a}_i\mathfrak{p}_i^m = 0$, e sia x un elemento non nullo in $\mathfrak{a}_i\mathfrak{p}_i^{m-1}$. Allora $\mathfrak{p}_i x = 0$, pertanto per un elemento x siffatto si ha $\mathrm{Ann}\,(x) \supseteq \mathfrak{p}_i$, e quindi $\mathrm{Ann}\,(x) = \mathfrak{p}_i$.

Viceversa, se $\mathrm{Ann}\,(x)$ è un ideale primo $\mathfrak{p}$, allora $r(\mathrm{Ann}\,(x)) = \mathfrak{p}$ e dunque, in virtú di (4.5), $\mathfrak{p}$ è un ideale primo appartenente a (0). ∎

Esercizi

1. Sia A un anello non noetheriano e sia Σ l'insieme degli ideali di A che non sono finitamente generati. Provare che Σ possiede elementi massimali e che gli elementi massimali di Σ sono ideali primi. [Sia $\mathfrak{a}$ un elemento massimale di Σ, e supponiamo che esistono elementi $x, y \in A$ tali che $x \notin \mathfrak{a}, y \notin \mathfrak{a}$ e $xy \in \mathfrak{a}$. Provare che esiste un ideale finitamente generato $\mathfrak{a}_0 \subseteq \mathfrak{a}$ tale che $\mathfrak{a}_0 + (x) = \mathfrak{a} + (x)$, e che $\mathfrak{a} = \mathfrak{a}_0 + x \quad (\mathfrak{a}:x)$. Poiché $(\mathfrak{a}:x)$ contiene propriamente $\mathfrak{a}$, esso è finitamente generato e pertanto tale risulta $\mathfrak{a}$.]

   Dunque un anello in cui ogni ideale primo è finitamente generato è noetheriano (I. S. Cohen).

2. Sia A un anello noetheriano e sia $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$. Dimostrare che f è nilpotente se e soltanto se ciascun a_n è nilpotente.

3. Sia $\mathfrak{a}$ un ideale irriducibile in un anello A. Allora le seguenti condizioni sono equivalenti:
   i) $\mathfrak{a}$ è primario;
   ii) per ogni parte moltiplicativa S di A si ha $(S^{-1}\mathfrak{a})^c = (\mathfrak{a}:x)$ per qualche $x \in S$;
   iii) la successione $(\mathfrak{a}:x^n)$ è stazionaria, per ogni $x \in A$.

4. Quali dei seguenti anelli sono noetheriani?

i) L'anello delle funzioni razionali di z prive di poli sulla circonferenza $|z| = 1$.
ii) L'anello delle serie di potenze in z con un raggio di convergenza positivo.
iii) L'anello delle serie di potenze in z con un raggio di convergenza infinito.
iv) L'anello dei polinomi in z le cui prime k derivate si annullano nell'origine (essendo k un intero fissato).
v) L'anello dei polinomi in z, w tali che tutte le derivate parziali rispetto a w si annullano per $z = 0$.
In tutti i casi considerati i coefficienti sono numeri complessi.

5. Sia A un anello noetheriano, B una A-algebra finitamente generata, G un gruppo finito di A-automorfismi di B, e B^G l'insieme di tutti gli elementi di B che sono lasciati fissi da ogni elemento di G. Provare che B^G è una A-algebra finitamente generata.

6. Se un anello finitamente generato K è un campo, esso è un campo finito.
[Se K ha caratteristica 0, si ha $\mathbf{Z} \subset \mathbf{Q} \subseteq K$. Poiché K è finitamente generato sopra $\mathbf{Z}$ esso è finitamente generato sopra $\mathbf{Q}$, dunque, in virtú di (7.9), K è un $\mathbf{Q}$-modulo finitamente generato. Applicare ora (7.8) per ottenere una contraddizione. Ne segue che K è di caratteristica $p > 0$, sicché è una $\mathbf{Z}/(p)$-algebra finitamente generata. Utilizzare (7.9) per completare la dimostrazione.]

7. Sia X una varietà algebrica affine definita da una famiglia di equazioni $f_\alpha(t_1, \ldots, t_n) = 0$ $(\alpha \in I)$ (Capitolo 1, Esercizio 27). Dimostrare che esiste un sottoinsieme finito I_0 di I tale che X è definita dalle equazioni $f_\alpha(t_1, \ldots, t_n) = 0$ per $\alpha \in I_0$.

8. Se $A[x]$ è noetheriano, A risulta necessariamente noetheriano?

9. Sia A un anello tale che
(1) per ogni ideale massimale $\mathfrak{m}$ di A, l'anello locale $A_\mathfrak{m}$ è noetheriano;
(2) per ogni elemento $x \neq 0$ di A, l'insieme degli ideali massimali di A che contengono x è finito.

Dimostrare che A è noetheriano.
[Sia $\mathfrak{a} \neq 0$ un ideale di A. Siano $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ gli ideali massimali che contengono $\mathfrak{a}$. Scegliamo un elemento $x_0 \neq 0$ in $\mathfrak{a}$, e siano $\mathfrak{m}_1, \ldots, \mathfrak{m}_{r+s}$ gli ideali massimali che contengono x_0. Poiché $\mathfrak{m}_{r+1}, \ldots, \mathfrak{m}_{r+s}$ non contengono $\mathfrak{a}$, esistono elementi $x_j \in \mathfrak{a}$ tali che $x_j \notin \mathfrak{m}_{r+j}$ $(1 \leqslant j \leqslant s)$. Inoltre, poiché $A_{\mathfrak{m}_i}$ $(1 \leqslant i \leqslant r)$ è noetheriano, l'estensione di $\mathfrak{a}$ in $A_{\mathfrak{m}_i}$ è un ideale finitamente generato.

Dunque esistono elementi $x_{s+1}, \ldots, x_t$ in $\mathfrak{a}$, le cui immagini in $A_{\mathfrak{m}_i}$ generano $A_{\mathfrak{m}_i}\mathfrak{a}$ per $i = 1, \ldots, r$. Poniamo $\mathfrak{a}_0 = (x_0, \ldots, x_t)$. Dimostrare che $\mathfrak{a}_0$ e $\mathfrak{a}$ hanno la medesima estensione in $A_\mathfrak{m}$ per ogni ideale massimale $\mathfrak{m}$, e dedurre, in virtú di (3.9), che $\mathfrak{a}_0 = \mathfrak{a}$.]

10. Sia M un A-modulo noetheriano. Provare che $M[x]$ (Capitolo 2, Esercizio 6) è un $A[x]$-modulo noetheriano.

11. Sia A un anello tale che ogni anello locale $A_\mathfrak{p}$ è noetheriano. Allora A risulta necessariamente noetheriano?

12. Sia A un anello e B una A-algebra fedelmente piatta (Capitolo 3, Esercizio 16). Se B è noetheriano, provare che A è noetheriano. [Utilizzare la condizione della catena ascendente.]

13. Sia $f\colon A \to B$ un omomorfismo di anelli di tipo finito e sia $f^*\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ l'applicazione associata a f. Dimostrare che le fibre di f^* sono sottospazi noetheriani di B.

Teorema degli zeri (forma forte)

14. Sia k un campo algebricamente chiuso, A l'anello dei polinomi $k[t_1, \ldots, t_n]$, e sia $\mathfrak{a}$ un ideale di A. Sia V la varietà di k^n definita dall'ideale $\mathfrak{a}$, sicché V è l'insieme di tutti i punti $x = (x_1, \ldots, x_n) \in k^n$ tali che $f(x) = 0$ per ogni $f \in \mathfrak{a}$. Sia $I(V)$ l'ideale di V, ossia l'ideale di tutti i polinomi $g \in A$ tali che $g(x) = 0$ per ogni $x \in V$. Allora $I(V) = r(\mathfrak{a})$.
[È chiaro che $r(\mathfrak{a}) \subseteq I(V)$. Viceversa, se $f \notin r(\mathfrak{a})$, allora esiste un ideale primo $\mathfrak{p}$ contenente $\mathfrak{a}$ tale che $f \notin \mathfrak{p}$. Sia $\bar{f}$ l'immagine di f in $B = A/\mathfrak{p}$, $C = B_{\bar{f}} = B[1/\bar{f}]$, e sia $\mathfrak{m}$ un ideale massimale di C. Poiché C è una k-algebra finitamente generata si ha $C/\mathfrak{m} \cong k$, in virtú di (7.9). Le immagini x_i in $C/\mathfrak{m}$ dei generatori t_i di A definiscono cosí un punto $x = (x_1, \ldots, x_n) \in k^n$, e la costruzione mostra che $x \in V$ e $f(x) \neq 0$.]

15. Sia A un anello locale noetheriano, $\mathfrak{m}$ il suo ideale massimale e k il suo campo residuo, e sia M un A-modulo finitamente generato. Allora le seguenti condizioni sono equivalenti:
    i) M è libero;
    ii) M è piatto;
    iii) l'applicazione di $\mathfrak{m} \otimes M$ in $A \otimes M$ è iniettiva;
    iv) $\operatorname{Tor}_1^A(k, M) = 0$.

    [Per provare che iv) $\Rightarrow$ i), siano $x_1, \ldots, x_n$ elementi di M tali che le loro immagini in $M/\mathfrak{m}M$ formano una k-base di tale spazio vettoriale. In virtú di (2.8), gli x_i generano M. Sia F un A-modulo libero con base $e_1, \ldots, e_n$ e definiamo un omomorfismo $\phi\colon F \to M$ ponendo $\phi(e_i) = x_i$. Sia $E = \mathrm{Ker}\,(\phi)$. Allora la successione esatta $0 \to E \to F \to M \to 0$ fornisce una successione esatta

$$0 \to k \otimes_A E \to k \otimes_A F \xrightarrow{1\otimes\phi} k \otimes_A M \to 0.$$

Poiché $k \otimes F$ e $k \otimes M$ sono spazi vettoriali aventi la medesima dimensione sopra k, si ha che $1 \otimes \phi$ è un isomorfismo, sicché $k \otimes E = 0$, dunque $E = 0$ in virtú del lemma di Nakayama (E è finitamente generato, giacché è un sottomodulo di F, e A è noetheriano).]

16. Sia A un anello noetheriano, M un A-modulo finitamente generato. Allora le seguenti condizioni sono equivalenti:
 i) M è un A-modulo piatto;
 ii) $M_\mathfrak{p}$ è un $A_\mathfrak{p}$-modulo libero, per ogni ideale primo $\mathfrak{p}$;
 iii) $M_\mathfrak{m}$ è un $A_\mathfrak{m}$-modulo libero, per ogni ideale massimale $\mathfrak{m}$.

 In altre parole, piatto = localmente libero. [Utilizzare l'Esercizio 15.]

17. Sia A un anello e M un A-modulo noetheriano. Provare (imitando le dimostrazioni di (7.11) e (7.12)) che ogni sottomodulo N di M possiede una decomposizione primaria (Capitolo 4, Esercizi 20-23).

18. Sia A un anello noetheriano, $\mathfrak{p}$ un ideale primo di A, e M un A-modulo finitamente generato. Dimostrare che le seguenti condizioni sono equivalenti:
 i) $\mathfrak{p}$ appartiene a 0 in M;
 ii) esiste un elemento $x \in M$ tale che $\mathrm{Ann}\,(x) = \mathfrak{p}$;
 iii) esiste un sottomodulo di M isomorfo ad $A/\mathfrak{p}$.

 Dedurre che esiste una catena di sottomoduli

$$0 = M_0 \subset M_1 \subset \quad \subset M_r = M$$

tale che ciascun quoziente M_i/M_{i-1} è della forma $A/\mathfrak{p}_i$, dove $\mathfrak{p}_i$ è un ideale primo di A.

19. Sia $\mathfrak{a}$ un ideale in un anello noetheriano A. Siano

$$\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i = \bigcap_{j=1}^{s} \mathfrak{c}_j$$

due decomposizioni minimali di $\mathfrak{a}$ come intersezione di ideali *irriducibili*. Dimostrare che $r = s$ e che (a meno di un eventuale cambiamento di indici) $r(\mathfrak{b}_i) = r(\mathfrak{c}_i)$ per ogni i.

[Provare che per ciascun $i = 1, \ldots, r$ esiste un indice j tale che

$$\mathfrak{a} = \mathfrak{b}_1 \cap \quad \cap \mathfrak{b}_{i-1} \cap \mathfrak{c}_j \cap \mathfrak{b}_{i+1} \cap \quad \cap \mathfrak{b}_r.]$$

Enunciare e dimostrare un risultato analogo per i moduli.

20. Sia X uno spazio topologico e sia $\mathscr{F}$ la più piccola famiglia di sottoinsiemi di X che contiene tutti gli aperti di X ed è chiusa rispetto alle intersezioni finite e alla formazione del complementare.
    i) Provare che un sottoinsieme E di X appartiene a $\mathscr{F}$ se e soltanto se E è un'unione finita di insiemi della forma $U \cap C$, dove U è aperto e C è chiuso.
    ii) Supponiamo che X sia irriducibile e sia $E \in \mathscr{F}$. Provare che E è denso in X (ossia, che $\bar{E} = X$) se e soltanto se E contiene un aperto non vuoto di X.

21. Sia X uno spazio topologico noetheriano (Capitolo 6, Esercizio 5) e sia $E \subseteq X$. Dimostrare che $E \in \mathscr{F}$ se e soltanto se, per ogni chiuso irriducibile $X_0 \subseteq X$, o $\overline{E \cap X_0} \neq X_0$ oppure $E \cap X_0$ contiene un aperto non vuoto di X_0. [Supponiamo che $E \notin \mathscr{F}$. Allora la famiglia dei chiusi $X' \subseteq X$ tali che $E \cap X' \notin \mathscr{F}$ è non vuota e pertanto possiede un elemento minimale X_0. Provare che X_0 è irriducibile e successivamente che ciascuna delle alternative di cui sopra porta a concludere che $E \cap X_0 \in \mathscr{F}$.]
    Gli insiemi appartenenti a $\mathscr{F}$ prendono il nome di sottoinsiemi *costruibili* di X.

22. Sia X uno spazio topologico noetheriano e sia E un sottoinsieme di X. Dimostrare che E è aperto in X se, e soltanto se, per ogni chiuso irriducibile X_0 di X, o $E \cap X_0 = \emptyset$ oppure $E \cap X_0$ contiene un aperto non vuoto di X_0. [La dimostrazione è simile a quella dell'Esercizio 21.]

23. Sia A un anello noetheriano, $f: A \to B$ un omomorfismo di anelli di tipo finito (sicché B è noetheriano). Poniamo $X = \operatorname{Spec}(A)$, $Y = \operatorname{Spec}(B)$ e sia $f^*: Y \to X$ l'applicazione associata a f. Allora l'immagine mediante f^* di un sottoinsieme costruibile E di Y è un sottoinsieme costruibile di X.
    [In virtù dell'Esercizio 20, basta prendere $E = U \cap C$ dove U è aperto e C è chiuso in Y; allora, sostituendo B con un'immagine omomorfa, ci riduciamo al caso in cui E è aperto in Y. Poiché Y è noetheriano, E è quasi-compatto e pertanto è un'unione finita di aperti della forma $\operatorname{Spec}(B_g)$. Dunque ci riduciamo al caso in cui $E = Y$. Per provare che $f^*(Y)$ è costruibile, utilizziamo il criterio dell'Esercizio 21. Sia X_0 un chiuso irriducibile di X tale che

$f^*(Y) \cap X_0$ è denso in X_0. Si ha $f^*(Y) \cap X_0 = f^*(f^{*-1}(X_0))$, e $f^{*-1}(X_0) = \text{Spec}\,((A/\mathfrak{p}) \otimes_A B)$, dove $X_0 = \text{Spec}\,(A/\mathfrak{p})$. Dunque ci riduciamo al caso in cui A è un dominio di integrità e f è iniettivo. Se $Y_1, \ldots, Y_n$ sono le componenti irriducibili di Y, basta provare che qualche sottoinsieme $f^*(Y_i)$ contiene un aperto non vuoto di X. Cosí finalmente siamo ricondotti al caso in cui A, B sono domini di integrità e f è iniettivo (e ancora di tipo finito); ora basta utilizzare l'Esercizio 21 del Capitolo 5 per completare la dimostrazione.]

24. Con le notazioni e le ipotesi dell'Esercizio 23, f^* è un'applicazione aperta $\Leftrightarrow$ f ha la proprietà del going-down (Capitolo 5, Esercizio 10). [Supponiamo che f abbia la proprietà del going-down. Come si è visto nell'Esercizio 23, ci riduciamo a provare che $E = f^*(Y)$ è aperto in X. La proprietà del going-down asserisce che se $\mathfrak{p} \in E$ e $\mathfrak{p}' \subseteq \mathfrak{p}$, allora $\mathfrak{p}' \in E$: in altre parole, che se X_0 è un chiuso irriducibile di X e X_0 incontra E, allora $E \cap X_0$ è denso in X_0. Ma allora, in virtú degli Esercizi 20 e 22, E è aperto in X.]

25. Sia A noetheriano, $f: A \to B$ un omomorfismo di tipo finito e *piatto* (ossia, B è piatto come A-modulo). Allora $f^*: \text{Spec}\,(B) \to \text{Spec}\,(A)$ è un'applicazione aperta. [Cfr. l'Esercizio 24, e l'Esercizio 11 del Capitolo 5.]

Gruppo di Grothendieck

26. Sia A un anello noetheriano e denotiamo con $F(A)$ l'insieme di tutte le classi di isomorfismo di A-moduli finitamente generati. Sia C il gruppo abeliano libero generato da $F(A)$. A ciascuna successione esatta corta $0 \to M' \to M \to M'' \to 0$ di A-moduli finitamente generati associamo l'elemento $(M') - (M) + (M'')$ di C, dove (M) è la classe di isomorfismo di M, ecc.... Sia D il sottogruppo di C generato da tali elementi, per ogni successione esatta corta. Il gruppo quoziente C/D è chiamato il *gruppo di Grothendieck* di A, e si denota con $K(A)$. Se M è un A-modulo finitamente generato, denotiamo con $\gamma(M)$, o con $\gamma_A(M)$, l'immagine di (M) in $K(A)$.

    i) Provare che $K(A)$ possiede la seguente proprietà universale: per ogni funzione additiva λ sulla classe degli A-moduli finitamente generati, a valori in un gruppo abeliano G, esiste uno ed un solo omomorfismo $\lambda_0: K(A) \to G$ tale che $\lambda(M) = \lambda_0(\gamma(M))$ per ogni M.

ii) Provare che $K(A)$ è generato dagli elementi $\gamma(A/\mathfrak{p})$, dove $\mathfrak{p}$ è un ideale primo di A. [Utilizzare l'Esercizio 18.]

iii) Se A è un campo, o piú in generale se A è un dominio a ideali principali, allora $K(A) \cong \mathbf{Z}$.

iv) Sia $f: A \to B$ un omomorfismo di anelli *finito*. Dimostrare che la restrizione degli scalari dà origine ad un omomorfismo $f_!: K(B) \to K(A)$ tale che $f_!(\gamma_B(N)) = \gamma_A(N)$ per un B-modulo N. Se $g: B \to C$ è un altro omomorfismo di anelli finito, provare che $(g \circ f)_! = f_! \circ g_!$.

27. Sia A un anello noetheriano e sia $F_1(A)$ l'insieme di tutte le classi di isomorfismo di A-moduli *piatti* finitamente generati. Ripetendo la costruzione dell'Esercizio 26 si ottiene un gruppo $K_1(A)$. Denotiamo con $\gamma_1(M)$ l'immagine di (M) in $K_1(A)$.

i) Provare che il prodotto tensoriale di moduli sopra A induce una struttura di anello commutativo su $K_1(A)$, tale che $\gamma_1(M) \cdot \gamma_1(N) = \gamma_1(M \otimes N)$. L'elemento unità di tale anello è $\gamma_1(A)$.

ii) Dimostrare che il prodotto tensoriale induce una struttura di $K_1(A)$-modulo sul gruppo $K(A)$, tale che $\gamma_1(M) \quad \gamma(N) = \gamma(M \otimes N)$.

iii) Se A è un anello locale (noetheriano), allora $K_1(A) \cong \mathbf{Z}$.

iv) Sia $f: A \to B$ un omomorfismo di anelli, B essendo noetheriano. Dimostrare che l'estensione degli scalari dà origine ad un omomorfismo di anelli $f^!: K_1(A) \to K_1(B)$ tale che $f^!(\gamma_1(M)) = \gamma_1(B \otimes_A M)$.
[Se M è piatto e finitamente generato sopra A, allora $B \otimes_A M$ è piatto e finitamente generato sopra B.] Se $g: B \to C$ è un altro omomorfismo di anelli (con C noetheriano), allora $(f \circ g)^! = f^! \circ g^!$.

v) Se $f: A \to B$ è un omomorfismo di anelli finito, allora

$$f_!(f^!(x)y) = xf_!(y)$$

per $x \in K_1(A), y \in K(B)$. In altre parole, considerando $K(B)$ come un $K_1(A)$-modulo mediante restrizione degli scalari, l'omomorfismo $f_!$ è un omomorfismo di $K_1(A)$-moduli.

Osservazione. Poiché $F_1(A)$ è un sottoinsieme di $F(A)$, si ha un omomorfismo di gruppi $\varepsilon: K_1(A) \to K(A)$, dato da $\varepsilon(\gamma_1(M)) = \gamma(M)$. Se l'anello A ha dimensione finita ed è *regolare*, ossia, se tutti i suoi anelli locali $A_\mathfrak{p}$ sono regolari (Capitolo 11), si può dimostrare che ε è un isomorfismo.

Anelli artiniani

Un *anello artiniano* è un anello che soddisfa la d.c.c. (o in modo equivalente, la condizione minimale) sugli ideali.

L'apparente simmetria con gli anelli noetheriani trae tuttavia in inganno. Infatti proveremo che un anello artiniano è necessariamente noetheriano e di un tipo molto particolare. In un certo senso un anello artiniano è il tipo più semplice di anello dopo un campo, e noi studiamo tali anelli non per la loro generalità, ma per la loro semplicità.

Proposizione 8.1. *In un anello artiniano A ogni ideale primo è massimale.*

Dimostrazione. Sia $\mathfrak{p}$ un ideale primo di A. Allora $B = A/\mathfrak{p}$ è un dominio di integrità artiniano. Sia $x \in B$, $x \neq 0$. In virtú della d.c.c. si ha $(x^n) = (x^{n+1})$ per qualche intero $n > 0$, da cui $x^n = x^{n+1}y$ per qualche $y \in B$. Poiché B è un dominio di integrità e $x \neq 0$, ne segue che si può cancellare x^n, sicché $xy = 1$. Dunque x possiede un inverso in B, e pertanto B è un campo, e quindi $\mathfrak{p}$ è un ideale massimale. ∎

Corollario 8.2. *In un anello artiniano il nilradicale coincide con il radicale di Jacobson.* ∎

Proposizione 8.3. *Un anello artiniano possiede soltanto un numero finito di ideali massimali.*

Dimostrazione. Consideriamo l'insieme di tutte le intersezioni finite $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r$, dove gli $\mathfrak{m}_i$ sono ideali massimali. Tale insieme possiede un elemento minimale, diciamo $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$; dunque, per un arbitrario ideale massimale $\mathfrak{m}$, si ha $\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$, e pertanto $\mathfrak{m} \supseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. In virtú di (1.11) $\mathfrak{m} \supseteq \mathfrak{m}_i$ per qualche i, sicché $\mathfrak{m} = \mathfrak{m}_i$, poiché $\mathfrak{m}_i$ è massimale. ∎

Proposizione 8.4. *In un anello artiniano il nilradicale $\mathfrak{N}$ è nilpotente.*

Dimostrazione. In virtú della d.c.c. si ha $\mathfrak{N}^k = \mathfrak{N}^{k+1} = \ldots = \mathfrak{a}$, diciamo, per qualche intero $k > 0$. Supponiamo che $\mathfrak{a} \neq 0$, e denotiamo con Σ l'insieme di tutti gli ideali $\mathfrak{b}$ tali che $\mathfrak{a}\mathfrak{b} \neq 0$. Allora Σ è non vuoto, giacché $\mathfrak{a} \in \Sigma$. Sia $\mathfrak{c}$ un elemento minimale di Σ; allora esiste un elemento $x \in \mathfrak{c}$ tale che $x\mathfrak{a} \neq 0$; si ha $(x) \subseteq \mathfrak{c}$, da cui $(x) = \mathfrak{c}$, stante la minimalità di $\mathfrak{c}$. Ma $(x\mathfrak{a})\mathfrak{a} = x\mathfrak{a}^2 = x\mathfrak{a} \neq 0$, e $x\mathfrak{a} \subseteq (x)$, da cui $x\mathfrak{a} = (x)$ (ancora per la minimalità di $\mathfrak{c}$). Dunque $x = xy$ per qualche $y \in \mathfrak{a}$, e pertanto $x = xy = xy^2 = \quad = xy^n = \ldots$. Ma $y \in \mathfrak{a} = \mathfrak{N}^k \subseteq \mathfrak{N}$, sicché y è nilpotente e pertanto $x = xy^n = 0$. Ciò contraddice la scelta di x, e pertanto $\mathfrak{a} = 0$. ■

Dicesi *catena* di ideali primi di un anello A una successione finita strettamente crescente $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \quad \subset \mathfrak{p}_n$; la *lunghezza* della catena è n. Si definisce *dimensione* di A l'estremo superiore delle lunghezze di tutte le catene di ideali primi in A; essa è un intero $\geqslant 0$, oppure è $+\infty$ (supponendo $A \neq 0$). Un campo ha dimensione zero; l'anello $\mathbf{Z}$ ha dimensione 1.

Teorema 8.5. *Un anello A è artiniano $\Leftrightarrow$ A è noetheriano e* $\dim A = 0$.

Dimostrazione. $\Rightarrow$: In virtú di (8.1) si ha $\dim A = 0$. Siano $\mathfrak{m}_i$ $(1 \leqslant i \leqslant n)$ gli ideali massimali distinti di A (cfr. (8.3)). Allora $\prod_{i=1}^{n} \mathfrak{m}_i^k \subseteq (\bigcap_{i=1}^{n} \mathfrak{m}_i)^k = \mathfrak{N}^k = 0$. Dunque, in virtú di (6.11), A è noetheriano.

$\Leftarrow$: Poiché l'ideale zero ha una decomposizione primaria (cfr. (7.13)), A possiede soltanto un numero finito di ideali primi minimali, e questi sono tutti massimali poiché $\dim A = 0$. Ne segue che $\mathfrak{N} = \bigcap_{i=1}^{n} \mathfrak{m}_i$, diciamo; si ha $\mathfrak{N}^k = 0$ in virtú di (7.15), da cui $\prod_{i=1}^{n} \mathfrak{m}_i^k = 0$, come si è visto nella prima parte della dimostrazione. Dunque, in virtú di (6.11), A è un anello artiniano. ■

Se A è un anello locale artiniano con ideale massimale $\mathfrak{m}$, allora $\mathfrak{m}$ è l'unico ideale primo di A e pertanto $\mathfrak{m}$ è il nilradicale di A. Ne segue che ogni elemento di $\mathfrak{m}$ è nilpotente, e $\mathfrak{m}$ stesso è nilpotente. Ogni elemento di A o è invertibile oppure è nilpotente. Un esempio di anello siffatto è $\mathbf{Z}/(p^n)$, dove p è un numero primo e $n \geqslant 1$.

Proposizione 8.6. *Sia A un anello locale noetheriano, $\mathfrak{m}$ il suo ideale massimale. Allora vale una soltanto delle due seguenti affermazioni*:

i) $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ *per ogni* n;

ii) $\mathfrak{m}^n = 0$ *per qualche* n, *nel qual caso A è un anello locale artiniano.*

Dimostrazione. Supponiamo che $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ per qualche n. In virtú del lemma di Nakayama (cfr. (2.6)) si ha $\mathfrak{m}^n = 0$. Sia $\mathfrak{p}$ un ideale primo arbitrario di A. Allora $\mathfrak{m}^n \subseteq \mathfrak{p}$, da cui (prendendo i radicali) $\mathfrak{m} = \mathfrak{p}$. Dunque $\mathfrak{m}$ è l'unico ideale primo di A e pertanto A è artiniano. ∎

Teorema 8.7. (Teorema di struttura per gli anelli artiniani). *Un anello artiniano A risulta in modo unico (a meno di isomorfismi) un prodotto diretto finito di anelli locali artiniani.*

Dimostrazione. Siano $\mathfrak{m}_i$ $(1 \leqslant i \leqslant n)$ gli ideali massimali distinti di A. Dalla dimostrazione di (8.5) si ha $\prod_{i=1}^{n} \mathfrak{m}_i^k = 0$ per qualche intero $k > 0$. In virtú di (1.16) gli ideali $\mathfrak{m}_i^k$ sono a due a due coprimi, sicché $\bigcap \mathfrak{m}_i^k = \prod \mathfrak{m}_i^k$, stante (1.10). Ne segue, ancora in virtú di (1.10), che l'applicazione naturale $A \to \prod_{i=1}^{n} (A/\mathfrak{m}_i^k)$ è un isomorfismo. Ciascun $A/\mathfrak{m}_i^k$ è un anello locale artiniano, dunque A è un prodotto diretto di anelli locali artiniani.

Viceversa, supponiamo che $A \cong \prod_{i=1}^{m} A_i$, dove gli A_i sono anelli locali artiniani. Allora, per ogni indice i si ha un omomorfismo suriettivo naturale (proiezione sull'i-esimo fattore) $\phi_i \colon A \to A_i$. Poniamo $\mathfrak{a}_i = \operatorname{Ker}(\phi_i)$. In virtú di (1.10) gli $\mathfrak{a}_i$ sono a due a due coprimi, e $\bigcap \mathfrak{a}_i = 0$. Sia $\mathfrak{q}_i$ l'unico ideale primo di A_i, e sia $\mathfrak{p}_i$ la sua contrazione $\phi_i^{-1}(\mathfrak{q}_i)$. L'ideale $\mathfrak{p}_i$ è primo e quindi massimale, stante (8.1). Poiché $\mathfrak{q}_i$ è nilpotente, si ha che $\mathfrak{a}_i$ è $\mathfrak{p}_i$-primario, e quindi $\bigcap \mathfrak{a}_i = (0)$ è una decomposizione primaria dell'ideale zero in A. Poiché gli $\mathfrak{a}_i$ sono a due a due coprimi, tali risultano i $\mathfrak{p}_i$, e pertanto essi sono ideali primi isolati di (0). Ne segue che tutte le componenti primarie $\mathfrak{a}_i$ sono isolate, e pertanto univocamente determinate da A, in virtú del II teorema di unicità (4.11). Dunque gli anelli $A_i \cong A/\mathfrak{a}_i$ sono univocamente determinati da A. ∎

Esempio. Un anello con un unico ideale primo non è necessariamente noetheriano (e quindi neppure artiniano). Sia $A = k[x_1, x_2, \ldots]$ l'anello dei polinomi in una infinità numerabile di indeterminate x_n sopra un campo k, e sia $\mathfrak{a}$ l'ideale $(x_1, x_2^2, \quad, x_n^n, \ldots)$. L'anello

$B = A/\mathfrak{a}$ possiede un unico ideale primo (precisamente l'immagine di $(x_1, x_2, \ldots, x_n, \ldots)$), dunque B è un anello locale di dimensione 0. Ma B non è noetheriano, giacché non è difficile vedere che il suo ideale primo non è finitamente generato.

Se A è un anello locale, $\mathfrak{m}$ il suo ideale massimale, $k = A/\mathfrak{m}$ il suo campo residuo, l'A-modulo $\mathfrak{m}/\mathfrak{m}^2$ è annullato da $\mathfrak{m}$ e pertanto ha la struttura di un k-spazio vettoriale. Se $\mathfrak{m}$ è finitamente generato (per es., se A è noetheriano), le immagini in $\mathfrak{m}/\mathfrak{m}^2$ di un sistema di generatori di $\mathfrak{m}$ generano $\mathfrak{m}/\mathfrak{m}^2$ come spazio vettoriale sopra k, e pertanto $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$ è finita. (Cfr. (2.8).)

Proposizione 8.8. *Sia A un anello locale artiniano. Allora le seguenti condizioni sono equivalenti:*

i) *ogni ideale di A è principale;*

ii) *l'ideale massimale $\mathfrak{m}$ è principale;*

iii) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \leqslant 1$.

Dimostrazione. È chiaro che i) $\Rightarrow$ ii) $\Rightarrow$ iii).

iii) $\Rightarrow$ i): Se $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 0$, allora $\mathfrak{m} = \mathfrak{m}^2$, da cui $\mathfrak{m} = 0$ in virtú del lemma di Nakayama (2.6), e pertanto A è un campo e non c'è nulla da dimostrare.

Se $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$, allora $\mathfrak{m}$ è un ideale principale in virtú di (2.8) (ponendo ivi $M = \mathfrak{m}$), diciamo $\mathfrak{m} = (x)$. Sia $\mathfrak{a}$ un ideale di A, distinto da (0) e (1). Si ha $\mathfrak{m} = \mathfrak{N}$, dunque $\mathfrak{m}$ è nilpotente in virtú di (8.4) e pertanto esiste un intero r tale che $\mathfrak{a} \subseteq \mathfrak{m}^r$, $\mathfrak{a} \nsubseteq \mathfrak{m}^{r+1}$; dunque esiste un elemento $y \in \mathfrak{a}$ tale che $y = ax^r$, $y \notin (x^{r+1})$; di conseguenza $a \notin (x)$ e a è invertibile in A. Ne segue che $x^r \in \mathfrak{a}$, pertanto $\mathfrak{m}^r = (x^r) \subseteq \mathfrak{a}$ e quindi $\mathfrak{a} = \mathfrak{m}^r = (x^r)$. Dunque $\mathfrak{a}$ è principale. ∎

Esempio. Gli anelli $\mathbf{Z}/(p^n)$ (p primo), $k[x]/(f^n)$ (f irriducibile) soddisfano le condizioni di (8.8). D'altra parte, l'anello locale artiniano $k[x^2, x^3]/(x^4)$ non soddisfa tali condizioni: in tal caso $\mathfrak{m}$ è generato da x^2 e x^3 (mod x^4), sicché chiaramente non è principale.

Esercizi

1. Sia $\mathfrak{q}_1 \cap \quad \cap\, \mathfrak{q}_n = 0$ una decomposizione primaria minimale dell'ideale zero in un anello noetheriano, e sia $\mathfrak{q}_i$ $\mathfrak{p}_i$-primario. Sia $\mathfrak{p}_i^{(r)}$ la *potenza simbolica* r-esima di $\mathfrak{p}_i$ (Capitolo 4, Esercizio 13).

Dimostrare che per ciascun indice $i = 1, \ldots, n$ esiste un intero r_i tale che $\mathfrak{p}_i^{(r_i)} \subseteq \mathfrak{q}_i$.

Supponiamo che $\mathfrak{q}_i$ sia una componente primaria isolata. Allora $A_{\mathfrak{p}_i}$ è un anello locale artiniano, sicché se $\mathfrak{m}_i$ è il suo ideale massimale, si ha $\mathfrak{m}_i^r = 0$ per ogni r abbastanza grande, da cui $\mathfrak{q}_i = \mathfrak{p}_i^{(r)}$ per ogni r abbastanza grande.

Se $\mathfrak{q}_i$ è una componente primaria immersa, allora $A_{\mathfrak{p}_i}$ *non* è artiniano, sicché le potenze $\mathfrak{m}_i^r$ sono tutte distinte e quindi gli ideali $\mathfrak{p}_i^{(r)}$ sono tutti distinti. Pertanto nella decomposizione primaria assegnata si può sostituire $\mathfrak{q}_i$ con uno qualsiasi degli infiniti ideali $\mathfrak{p}_i$-primari della forma $\mathfrak{p}_i^{(r)}$, con $r \geqslant r_i$, e quindi vi sono infinite decomposizioni primarie minimali di (0), le quali differiscono soltanto per la $\mathfrak{p}_i$-componente.

2. Sia A un anello noetheriano. Provare che le seguenti condizioni sono equivalenti:

   i) A è artiniano;
   ii) Spec (A) è discreto e finito;
   iii) Spec (A) è discreto.

3. Sia k un campo e A una k-algebra finitamente generata. Dimostrare che le seguenti condizioni sono equivalenti:

   i) A è artiniano;
   ii) A è una k-algebra finita.

   [Per provare che i) $\Rightarrow$ ii), utilizzare (8.7) per ridursi al caso in cui A è un anello locale artiniano. In virtú del teorema degli zeri, il campo residuo di A è un'estensione finita di k. Ora utilizzare il fatto che A è un A-modulo di lunghezza finita. Per provare che ii) $\Rightarrow$ i), osservare che gli ideali di A sono k-sottospazi vettoriali e pertanto soddisfano la d.c.c.]

4. Sia $f: A \to B$ un omomorfismo di anelli di tipo finito. Consideriamo le seguenti affermazioni:

   i) f è finito;
   ii) le fibre di f^* sono sottospazi discreti di Spec (B);
   iii) per ogni ideale primo $\mathfrak{p}$ di A, l'anello $B \otimes_A k(\mathfrak{p})$ è una $k(\mathfrak{p})$-algebra finita ($k(\mathfrak{p})$ è il campo residuo di $A_{\mathfrak{p}}$);
   iv) le fibre di f^* sono finite.

   Dimostrare che i) $\Rightarrow$ ii) $\Leftrightarrow$ iii) $\Rightarrow$ iv). [Utilizzare gli Esercizi 2 e 3.]

Se f è intero e le fibre di f^* sono finite, f risulta necessariamente finito?

5. Nell'Esercizio 16 del Capitolo 5, provare che X è un rivestimento finito di L (ossia, il numero dei punti di X che giacciono su un dato punto di L è finito e limitato).

6. Sia A un anello noetheriano e $\mathfrak{q}$ un ideale $\mathfrak{p}$-primario in A. Consideriamo le catene di ideali primari da $\mathfrak{q}$ a $\mathfrak{p}$. Dimostrare che tutte le catene siffatte hanno lunghezza finita e limitata, e che tutte le catene massimali hanno la medesima lunghezza.

Capitolo nono

Anelli di valutazione discreta e domini di Dedekind

Come si è detto in precedenza, la teoria algebrica dei numeri è una delle fonti storiche dell'algebra commutativa. In questo capitolo, prendiamo in esame il caso che interessa la teoria dei numeri, ossia i domini di Dedekind. Dedurremo la fattorizzazione unica degli ideali nei domini di Dedekind dai teoremi generali sulla decomposizione primaria. Sebbene un approccio diretto sia naturalmente possibile, si riesce a comprendere meglio, in tal modo, il contesto preciso della teoria dei numeri in algebra commutativa. Un'altra classe importante di domini di Dedekind si presenta in relazione con le curve algebriche non singolari. Infatti la rappresentazione geometrica della condizione di Dedekind è: varietà irriducibile non singolare di dimensione 1.

Il capitolo precedente trattava gli anelli noetheriani di dimensione 0. Qui partiamo considerando il caso successivo più semplice, precisamente i *domini di integrità* noetheriani di dimensione uno, ossia, i domini noetheriani in cui ogni ideale primo non nullo è massimale. Il primo risultato è che in un anello siffatto vale un teorema di fattorizzazione unica per gli ideali:

Proposizione 9.1. *Sia A un dominio noetheriano di dimensione* 1. *Allora ogni ideale non nullo $\mathfrak{a}$ in A può venire espresso in modo unico come un prodotto di ideali primari i cui radicali sono tutti distinti.*

Dimostrazione. Essendo A noetheriano, $\mathfrak{a}$ possiede una decomposizione primaria minimale $\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$, in virtú di (7.13), dove ciascun $\mathfrak{q}_i$ è, diciamo, $\mathfrak{p}_i$-primario. Poiché $\dim A = 1$ e A è un dominio di integrità, ogni ideale primo non nullo di A è massimale, sicché i $\mathfrak{p}_i$ sono ideali massimali distinti (giacché $\mathfrak{p}_i \supseteq \mathfrak{q}_i \supseteq \mathfrak{a} \neq 0$), e pertanto sono a due a due coprimi. Ne segue, in virtú di (1.16), che i $\mathfrak{q}_i$ sono a due a due coprimi e pertanto, stante (1.10), si ha: $\prod \mathfrak{q}_i = \bigcap \mathfrak{q}_i$. Dunque $\mathfrak{a} = \prod \mathfrak{q}_i$.

Viceversa, se $\mathfrak{a} = \prod \mathfrak{q}_i$, la medesima argomentazione mostra che $\mathfrak{a} = \bigcap \mathfrak{q}_i$; questa risulta una decomposizione primaria minimale di $\mathfrak{a}$, in cui ciascun $\mathfrak{q}_i$ è una componente primaria isolata, e pertanto è univocamente determinato, in virtú di (4.11). ∎

Sia A un dominio noetheriano di dimensione uno in cui ogni ideale primario è la potenza di un ideale primo. In virtú di (9.1), in un anello siffatto si ha la fattorizzazione unica di ideali non nulli in prodotti di ideali primi. Se si localizza A rispetto a un ideale primo non nullo $\mathfrak{p}$, si ottiene un anello locale $A_\mathfrak{p}$ che soddisfa alle stesse condizioni di A, e pertanto in $A_\mathfrak{p}$ ogni ideale non nullo risulta una potenza dell'ideale massimale. Tali anelli locali possono essere caratterizzati in altri modi.

Anelli di valutazione discreta

Sia K un campo. Una *valutazione discreta* su K è un'applicazione v di K^* su $\mathbf{Z}$ (dove $K^* = K - \{0\}$ è il gruppo moltiplicativo di K) tale che:

1) $v(xy) = v(x) + v(y)$, ossia, v è un *omomorfismo*;
2) $v(x + y) \geqslant \min (v(x), v(y))$.

L'insieme costituito da 0 e da tutti gli elementi $x \in K^*$ tali che $v(x) \geqslant 0$ è un anello, chiamato l'*anello di valutazione* di v. Esso è un anello di valutazione del campo K. Talvolta è opportuno estendere v all'intero campo K ponendo $v(0) = +\infty$.

Esempi. I due esempi fondamentali sono:

1) $K = \mathbf{Q}$. Fissato un numero primo arbitrario p, ogni elemento non nullo $x \in \mathbf{Q}$ può essere scritto in modo unico nella forma $p^a y$, dove $a \in \mathbf{Z}$ e il numeratore e il denominatore di y sono entrambi primi rispetto a p. Definiamo $v_p(x) = a$. L'anello di valutazione di v_p è l'anello locale $\mathbf{Z}_{(p)}$.

2) $K = k(x)$, dove k è un campo e x un'indeterminata. Prendiamo un arbitrario polinomio irriducibile $f \in k[x]$ e definiamo v_f esattamente come in 1). L'anello di valutazione di v_f è allora l'anello locale di $k[x]$ rispetto all'ideale primo (f).

Un dominio di integrità A prende il nome di *anello di valutazione discreta* se esiste una valutazione discreta v del suo campo delle frazioni K tale che A è l'anello di valutazione di v. In virtú di (5.18), A

è un anello locale, e il suo ideale massimale $\mathfrak{m}$ è l'insieme di tutti gli elementi $x \in K$ tali che $v(x) > 0$.

Se due elementi x, y di A hanno lo stesso valore, ossia se $v(x) = v(y)$, allora $v(xy^{-1}) = 0$ e pertanto $u = xy^{-1}$ è invertibile in A. Dunque $(x) = (y)$.

Se $\mathfrak{a} \neq 0$ è un ideale di A, esiste un minimo intero k tale che $v(x) = k$ per qualche $x \in \mathfrak{a}$. Ne segue che $\mathfrak{a}$ contiene ogni elemento $y \in A$ con $v(y) \geq k$ e pertanto gli unici ideali $\neq 0$ in A sono gli ideali $\mathfrak{m}_k = \{y \in A : v(y) \geq k\}$. Questi formano un'unica catena $\mathfrak{m} \supset \mathfrak{m}_2 \supset \mathfrak{m}_3 \supset \ldots$, e pertanto A è noetheriano.

Inoltre, poiché $v\colon K^* \to \mathbf{Z}$ è suriettiva, esiste un elemento $x \in \mathfrak{m}$ tale che $v(x) = 1$, e allora $\mathfrak{m} = (x)$, e $\mathfrak{m}_k = (x^k)$ $(k \geq 1)$. Ne segue che $\mathfrak{m}$ è l'unico ideale primo non nullo di A, e dunque A risulta un dominio locale noetheriano di dimensione uno, in cui ogni ideale non nullo è una potenza dell'ideale massimale. Ebbene molte di queste proprietà sono caratteristiche degli anelli di valutazione discreta.

Proposizione 9.2. *Sia A un dominio locale noetheriano di dimensione uno, $\mathfrak{m}$ il suo ideale massimale, $k = A/\mathfrak{m}$ il suo campo residuo. Allora le seguenti condizioni sono equivalenti:*

i) *A è un anello di valutazione discreta;*

ii) *A è integralmente chiuso;*

iii) *$\mathfrak{m}$ è un ideale principale;*

iv) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$;

v) *Ogni ideale non nullo è una potenza di $\mathfrak{m}$;*

vi) *Esiste un elemento $x \in A$ tale che ogni ideale non nullo è della forma (x^k), con $k \geq 0$.*

Dimostrazione. Facciamo innanzitutto due osservazioni:

(A) Se $\mathfrak{a}$ è un ideale $\neq 0$, (1), allora $\mathfrak{a}$ è $\mathfrak{m}$-primario e $\mathfrak{a} \supseteq \mathfrak{m}^n$ per qualche n. Infatti $r(\mathfrak{a}) = \mathfrak{m}$, poiché $\mathfrak{m}$ è l'unico ideale primo non nullo; a questo punto basta utilizzare (7.16).

(B) $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ per ogni $n \geq 0$. Ciò segue da (8.6).

i) $\Rightarrow$ ii) in virtú di (5.18).

ii) $\Rightarrow$ iii). Sia $a \in \mathfrak{m}$ e $a \neq 0$. In virtú dell'osservazione (A), esiste un intero n tale che $\mathfrak{m}^n \subseteq (a)$, $\mathfrak{m}^{n-1} \nsubseteq (a)$. Scegliamo un elemento $b \in \mathfrak{m}^{n-1}$ e $b \notin (a)$, e poniamo $x = a/b \in K$, il campo delle frazioni di A. Si ha $x^{-1} \notin A$ (giacché $b \notin (a)$), sicché x^{-1} non è intero su A, e pertanto, in virtú di (5.1), si ha $x^{-1}\mathfrak{m} \nsubseteq \mathfrak{m}$ (altrimenti, se $x^{-1}\mathfrak{m} \subseteq \mathfrak{m}$, $\mathfrak{m}$ sarebbe un $A[x^{-1}]$-modulo fedele, finitamente generato come A-

modulo). Ma $x^{-1}\mathfrak{m} \subseteq A$, stante la costruzione di x, sicché $x^{-1}\mathfrak{m} = A$ e pertanto $\mathfrak{m} = Ax = (x)$.

iii) $\Rightarrow$ iv). In virtú di (2.8) si ha $\dim_k (\mathfrak{m}/\mathfrak{m}^2) \leq 1$, e per l'osservazione (B), $\mathfrak{m}/\mathfrak{m}^2 \neq 0$.

iv) $\Rightarrow$ v). Sia $\mathfrak{a}$ un ideale $\neq (0), (1)$. Stante l'osservazione (A), si ha $\mathfrak{a} \supseteq \mathfrak{m}^n$ per qualche n; da (8.8) (applicato a $A/\mathfrak{m}^n$) segue che $\mathfrak{a}$ è una potenza di $\mathfrak{m}$.

v) $\Rightarrow$ vi). In virtú dell'osservazione (B), $\mathfrak{m} \neq \mathfrak{m}^2$, sicché esiste un elemento $x \in \mathfrak{m}, x \notin \mathfrak{m}^2$. Ma $(x) = \mathfrak{m}^r$ per ipotesi, dunque $r = 1$, $(x) = \mathfrak{m}$, $(x^k) = \mathfrak{m}^k$.

vi) $\Rightarrow$ i). È chiaro che $(x) = \mathfrak{m}$, sicché $(x^k) \neq (x^{k+1})$ stante l'osservazione (B). Dunque se a è un arbitrario elemento non nullo di A, si ha $(a) = (x^k)$ per un unico valore di k. Definiamo $v(a) = k$ ed estendiamo v a K^* definendo $v(ab^{-1}) = v(a) - v(b)$. Si verifica che v è ben definita ed è una valutazione discreta, e che A è l'anello di valutazione di v. ■

Domini di Dedekind

Teorema 9.3. *Sia A un dominio noetheriano di dimensione uno. Allora le seguenti condizioni sono equivalenti:*

i) *A è integralmente chiuso;*

ii) *Ogni ideale primario in A è una potenza di un ideale primo;*

iii) *Ogni anello locale $A_\mathfrak{p}$ ($\mathfrak{p} \neq 0$) è un anello di valutazione discreta.*

Dimostrazione. i) $\Leftrightarrow$ iii) in virtú di (9.2) e (5.13).

ii) $\Leftrightarrow$ iii). Basta utilizzare (9.2) e il fatto che gli ideali primari e le potenze di ideali si comportano bene rispetto alla localizzazione: (4.8), (3.11). ■

Un anello che soddisfa le condizioni di (9.3) prende il nome di *dominio di Dedekind.*

Corollario 9.4. *In un dominio di Dedekind ogni ideale non nullo possiede una fattorizzazione unica come prodotto di ideali primi.*

Dimostrazione. La tesi si ottiene utilizzando (9.1) e (9.3). ■

Esempi. 1) Un arbitrario dominio a ideali principali A. Infatti A è noetheriano (giacché ogni ideale è finitamente generato) e di dimensione uno (cfr. l'esempio 3 dopo (1.6)). Inoltre ogni anello locale

$A_\mathfrak{p}$ ($\mathfrak{p} \neq 0$) è un dominio a ideali principali, e quindi, in virtú di (9.2), è un anello di valutazione discreta; dunque A è un dominio di Dedekind, stante (9.3).

2) Sia K un campo di numeri algebrici (ossia, un'estensione algebrica finita di $\mathbf{Q}$). Il suo *anello degli interi* A è la chiusura integrale di $\mathbf{Z}$ in K. (Per esempio, se $K = \mathbf{Q}(i)$, allora $A = \mathbf{Z}[i]$, l'anello degli interi di Gauss.) Allora A è un dominio di Dedekind:

Teorema 9.5. *L'anello degli interi in un campo di numeri algebrici K è un dominio di Dedekind.*

Dimostrazione. K è un'estensione separabile di $\mathbf{Q}$ (poiché ha caratteristica zero), sicché, in virtú di (5.17), esiste una base $v_1, \ldots, v_n$ di K sopra $\mathbf{Q}$ tale che $A \subseteq \sum \mathbf{Z}v_j$. Dunque A è finitamente generato come $\mathbf{Z}$-modulo e pertanto è noetheriano. Inoltre A è integralmente chiuso in virtú di (5.5). Per completare la dimostrazione, occorre far vedere che ogni ideale primo non nullo $\mathfrak{p}$ di A è massimale, e ciò segue da (5.8) e (5.9): (5.9) mostra che $\mathfrak{p} \cap \mathbf{Z} \neq 0$, dunque $\mathfrak{p} \cap \mathbf{Z}$ è un ideale massimale di $\mathbf{Z}$ e pertanto $\mathfrak{p}$ è massimale in A, in virtú di (5.8). ■

Osservazione. Il teorema sulla fattorizzazione unica (9.4) fu dimostrato originariamente per gli anelli degli interi nei campi di numeri algebrici. I teoremi di unicità del Capitolo 4 possono essere considerati come generalizzazioni di tale risultato: le potenze di ideali primi vanno sostituite con ideali primari, e i prodotti con intersezioni.

Ideali frazionari

Sia A un dominio di integrità, K il suo campo delle frazioni. Un A-sottomodulo M di K è un *ideale frazionario* di A se $xM \subseteq A$ per qualche elemento $x \neq 0$ in A. In particolare, gli ideali "ordinari" (chiamati ora ideali *interi*) sono ideali frazionari (prendendo $x = 1$). Ogni elemento $u \in K$ genera un ideale frazionario, denotato con (u) o Au, e chiamato *principale*. Se M è un ideale frazionario, l'insieme di tutti gli elementi $x \in K$ tali che $xM \subseteq A$ si denota con $(A : M)$.

Ogni A-sottomodulo finitamente generato M di K è un ideale frazionario. Infatti, se M è generato da $x_1, \ldots, x_n \in K$, si può scrivere $x_i = y_i z^{-1}$ ($1 \leqslant i \leqslant n$) dove y_i e z sono in A, e allora $zM \subseteq A$. Viceversa, se A è noetheriano, ogni ideale frazionario è finitamente generato, poiché è della forma $x^{-1}\mathfrak{a}$ per qualche ideale intero $\mathfrak{a}$.

Un A-sottomodulo M di K è un *ideale invertibile* se esiste un sottomodulo N di K tale che $MN = A$. Il modulo N è allora unico e risulta uguale a $(A: M)$, poiché si ha $N \subseteq (A: M) = (A: M)MN \subseteq \subseteq AN = N$. Ne segue che M è finitamente generato, e pertanto è un ideale frazionario: infatti, poiché $M \quad (A: M) = A$, esistono elementi $x_i \in M$ e $y_i \in (A: M)$ $(1 \leqslant i \leqslant n)$ tali che $\sum x_i y_i = 1$, e quindi per ogni $x \in M$ si ha $x = \sum (y_i x) x_i$: ciascun coefficiente $y_i x \in A$, sicché M è generato da $x_1, \quad , x_n$.

È chiaro che ogni ideale frazionario principale non nullo (u) è invertibile, il suo inverso essendo (u^{-1}). Gli ideali invertibili formano un gruppo rispetto alla moltiplicazione, il cui elemento neutro è $A = (1)$.

L'invertibilità è una proprietà *locale*:

Proposizione 9.6. *Per un ideale frazionario M, le seguenti condizioni sono equivalenti:*

i) *M è invertibile;*

ii) *M è finitamente generato e, per ogni ideale primo $\mathfrak{p}$, $M_\mathfrak{p}$ è invertibile;*

iii) *M è finitamente generato e, per ogni ideale massimale $\mathfrak{m}$, $M_\mathfrak{m}$ è invertibile.*

Dimostrazione. i) $\Rightarrow$ ii): $A_\mathfrak{p} = (M \quad (A: M))_\mathfrak{p} = M_\mathfrak{p} \quad (A_\mathfrak{p}: M_\mathfrak{p})$ in virtú di (3.11) e (3.15) (poiché M è finitamente generato, essendo invertibile).

ii) $\Rightarrow$ iii) come al solito.

iii) $\Rightarrow$ i): Poniamo $\mathfrak{a} = M \quad (A: M)$, che è un ideale intero. Per ogni ideale massimale $\mathfrak{m}$ si ha $\mathfrak{a}_\mathfrak{m} = M_\mathfrak{m} \quad (A_\mathfrak{m}: M_\mathfrak{m})$ (in virtú di (3.11) e (3.15)) $= A_\mathfrak{m}$ poiché $M_\mathfrak{m}$ è invertibile. Dunque $\mathfrak{a} \nsubseteq \mathfrak{m}$. Di conseguenza $\mathfrak{a} = A$ e pertanto M è invertibile. ∎

Proposizione 9.7. *Sia A un dominio locale. Allora A è un anello di valutazione discreta $\Leftrightarrow$ ogni ideale frazionario non nullo di A è invertibile.*

Dimostrazione. $\Rightarrow$. Sia x un generatore dell'ideale massimale $\mathfrak{m}$ di A, e sia $M \neq 0$ un ideale frazionario. Allora esiste un elemento $y \in A$ tale che $yM \subseteq A$: dunque yM è un ideale intero, diciamo (x^r), e pertanto $M = (x^{r-s})$, dove $s = v(y)$.

$\Leftarrow$: Ogni ideale intero non nullo è invertibile e pertanto è finitamente generato, sicché A è noetheriano. Dunque basta provare che ogni ideale intero non nullo è una potenza di $\mathfrak{m}$. Supponiamo che ciò sia falso; sia Σ l'insieme degli ideali non nulli che non sono potenze di $\mathfrak{m}$, e sia $\mathfrak{a}$ un elemento massimale di Σ. Allora $\mathfrak{a} \neq \mathfrak{m}$, da cui $\mathfrak{a} \subset \mathfrak{m}$;

ne segue che $\mathfrak{m}^{-1}\mathfrak{a} \subset \mathfrak{m}^{-1}\mathfrak{m} = A$ è un ideale (intero) proprio, e $\mathfrak{m}^{-1}\mathfrak{a} \supseteq \mathfrak{a}$. Se $\mathfrak{m}^{-1}\mathfrak{a} = \mathfrak{a}$, allora $\mathfrak{a} = \mathfrak{m}\mathfrak{a}$ e quindi $\mathfrak{a} = 0$ in virtú del lemma di Nakayama (2.6); pertanto $\mathfrak{m}^{-1}\mathfrak{a} \supset \mathfrak{a}$, sicché $\mathfrak{m}^{-1}\mathfrak{a}$ è una potenza di $\mathfrak{m}$ (in virtú della massimalità di $\mathfrak{a}$). Dunque $\mathfrak{a}$ è una potenza di $\mathfrak{m}$, ciò che è una contraddizione. ∎

Il risultato "globale" corrispondente di (9.7) è il

Teorema 9.8. *Sia A un dominio di integrità. Allora A è un dominio di Dedekind $\Leftrightarrow$ ogni ideale frazionario non nullo di A è invertibile.*

Dimostrazione. $\Rightarrow$: Sia $M \neq 0$ un ideale frazionario. Poiché A è noetheriano, M è finitamente generato. Per ogni ideale primo $\mathfrak{p} \neq 0$, $M_\mathfrak{p}$ è un ideale frazionario $\neq 0$ dell'anello di valutazione discreta $A_\mathfrak{p}$, sicché è invertibile in virtú di (9.7). Dunque M è invertibile, in virtú di (9.6).

$\Leftarrow$: Ogni ideale intero non nullo è invertibile, dunque finitamente generato, sicché A è noetheriano. Proveremo che ogni $A_\mathfrak{p}$ ($\mathfrak{p} \neq 0$) è un anello di valutazione discreta. A tal fine basta far vedere che ogni ideale intero $\neq 0$ in $A_\mathfrak{p}$ è invertibile, e utilizzare poi (9.7). Sia $\mathfrak{b} \neq 0$ un ideale (intero) in $A_\mathfrak{p}$, e poniamo $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{b} \cap A$. Allora $\mathfrak{a}$ è invertibile, sicché $\mathfrak{b} = \mathfrak{a}_\mathfrak{p}$ è invertibile in virtú di (9.7). ∎

Corollario 9.9. *Se A è un dominio di Dedekind, gli ideali frazionari non nulli di A formano un gruppo rispetto alla moltiplicazione.* ∎

Tale gruppo prende il nome di *gruppo degli ideali* di A; lo denotiamo con I. Con questa terminologia, l'enunciato (9.4) afferma che I è un gruppo (abeliano) libero, generato dagli ideali primi non nulli di A.

Denotiamo con K^* il gruppo moltiplicativo del campo delle frazioni K di A. Ogni elemento $u \in K^*$ definisce un ideale frazionario (u), e l'applicazione $u \mapsto (u)$ è un omomorfismo $\phi: K^* \to I$. L'immagine P di ϕ è il gruppo degli ideali frazionari *principali*: il gruppo quoziente $H = I/P$ è chiamato il *gruppo delle classi di ideali* di A. Il nucleo U di ϕ è l'insieme di tutti gli elementi $u \in K^*$ tali che $(u) = (1)$, sicché è il *gruppo degli elementi invertibili* di A. Si ha una successione esatta

$$1 \to U \to K^* \to I \to H \to 1.$$

Osservazione. Per i domini di Dedekind che si presentano in teoria dei numeri, valgono alcuni teoremi classici relativi ai gruppi H e U. Sia K un campo di numeri algebrici e sia A il suo anello degli interi, il quale è un dominio di Dedekind, in virtú di (9.5). In tal caso:

1) H è un gruppo *finito*. Il suo ordine h è il *numero di classe* del campo K. Le seguenti condizioni sono equivalenti: (i) $h = 1$; (ii) $I = P$; (iii) A è un dominio a ideali principali; (iv) A è un dominio a fattorizzazione unica.

2) U è un gruppo abeliano *finitamente generato*. Più precisamente, è possibile specificare il numero dei generatori di U. Innanzitutto, gli elementi di ordine finito in U sono esattamente le radici dell'unità che si trovano in K, ed essi formano un gruppo ciclico finito W; U/W è privo di torsione. Il numero dei generatori di U/W si ottiene nel modo seguente: se $[K: \mathbf{Q}] = n$, vi sono n monomorfismi distinti $K \to \mathbf{C}$ (il campo dei numeri complessi). Di questi, r_1, diciamo, mandano K in $\mathbf{R}$, e i rimanenti si accoppiano (se α è uno di essi, allora $\omega \circ \alpha$ è un altro, dove ω è l'automorfismo di $\mathbf{C}$ definito ponendo $\omega(z) = \bar{z}$) in r_2 coppie, diciamo: dunque $r_1 + 2r_2 = n$. Il numero dei generatori di U/W è allora $r_1 + r_2 - 1$.

Le dimostrazioni di tali risultati fanno parte della teoria algebrica dei numeri e non dell'algebra commutativa: esse richiedono delle tecniche di natura differente rispetto a quelle usate in questo testo.

Esempi. 1) $K = \mathbf{Q}(\sqrt{-1})$; $n = 2, r_1 = 0, r_2 = 1, r_1 + r_2 - 1 = 0$. Gli unici elementi invertibili in $\mathbf{Z}[i] = A$ sono le quattro radici dell'unità ± 1, $\pm i$.

2) $K = \mathbf{Q}(\sqrt{2})$; $n = 2$, $r_1 = 2$, $r_2 = 0$, $r_1 + r_2 - 1 = 1$. $W = \{\pm 1\}$, e U/W è ciclico infinito. Infatti, gli elementi invertibili in $A = \mathbf{Z}[\sqrt{2}]$ sono $\pm(1 + \sqrt{2})^n$, dove n è un intero arbitrario.

Esercizi

1. Sia A un dominio di Dedekind, S una parte moltiplicativa di A. Dimostrare che $S^{-1}A$ risulta o un dominio di Dedekind oppure il campo delle frazioni di A.

   Supponiamo che $S \neq A - \{0\}$, e siano H, H' i gruppi delle classi di ideali di A e di $S^{-1}A$, rispettivamente. Provare che l'estensione di ideali induce un omomorfismo suriettivo $H \to H'$.

2. Sia A un dominio di Dedekind. Se $f = a_0 + a_1x + \ldots + a_nx^n$ è un polinomio a coefficienti in A, il *contenuto* di f è l'ideale $c(f) = (a_0, \ldots, a_n)$ in A. Dimostrare il *lemma di Gauss*, secondo cui $c(fg) = c(f)c(g)$. [Localizzare rispetto a ciascun ideale massimale.]

3. Un anello di valutazione (che non sia un campo) è noetheriano se e soltanto se è un anello di valutazione discreta.

4. Sia A un dominio locale che non sia un campo e in cui l'ideale massimale $\mathfrak{m}$ è principale e $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0$. Dimostrare che A è un anello di valutazione discreta.

5. Sia M un modulo finitamente generato sopra un dominio di Dedekind. Provare che M è piatto $\Leftrightarrow M$ è privo di torsione.
[Utilizzare l'Esercizio 13 del Capitolo 3 e l'Esercizio 16 del Capitolo 7.]

6. Sia M un modulo di torsione ($T(M) = M$) finitamente generato sopra un dominio di Dedekind A. Dimostrare che M può essere rappresentato in modo unico come somma diretta finita di moduli $A/\mathfrak{p}_i^{n_i}$, dove i $\mathfrak{p}_i$ sono ideali primi non nulli di A. [Per ogni ideale primo $\mathfrak{p} \neq 0$, $M_\mathfrak{p}$ è un $A_\mathfrak{p}$-modulo di torsione; utilizzare poi il teorema di struttura per i moduli sopra un dominio a ideali principali.]

7. Sia A un dominio di Dedekind e $\mathfrak{a} \neq 0$ un ideale di A. Provare che ogni ideale di $A/\mathfrak{a}$ è principale.
Dedurre che ogni ideale di A può essere generato al piú da due elementi.

8. Siano $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ tre ideali in un dominio di Dedekind. Dimostrare che

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c})$$
$$\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c}).$$

[Localizzare.]

9. (Il Teorema cinese dei resti). Siano $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideali e $x_1, \ldots, x_n$ elementi di un dominio di Dedekind A. Allora il sistema di congruenze $x \equiv x_i \pmod{\mathfrak{a}_i}$ $(1 \leqslant i \leqslant n)$ possiede una soluzione x in $A \Leftrightarrow x_i \equiv x_j \pmod{\mathfrak{a}_i + \mathfrak{a}_j}$, ogni volta che $i \neq j$.
[Ciò equivale ad affermare che la successione di A-moduli

$$A \xrightarrow{\phi} \bigoplus_{i=1}^{n} A/\mathfrak{a}_i \xrightarrow{\psi} \bigoplus_{i<j} A/(\mathfrak{a}_i + \mathfrak{a}_j)$$

è esatta, dove ϕ e ψ sono definiti nel modo seguente:
$\phi(x) = (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$; $\psi(x_1 + \mathfrak{a}_1, \ldots, x_n + \mathfrak{a}_n)$ ha come (i, j)-componente $x_i - x_j + \mathfrak{a}_i + \mathfrak{a}_j$. Per provare che tale successione è esatta basta far vedere che essa è esatta quando viene localizzata in ogni ideale primo $\mathfrak{p} \neq 0$: in altre parole possiamo supporre che A è un anello di valutazione discreta, e allora si conclude facilmente.]

Capitolo decimo

Completamenti

Nella geometria algebrica classica (ossia, sul campo dei numeri complessi) si possono utilizzare metodi trascendenti. Ciò significa che si riguarda una funzione razionale come una funzione analitica (di una o piú variabili complesse) e si considera il suo sviluppo in serie di potenze nell'intorno di un punto. In geometria algebrica astratta la cosa migliore che si può fare è considerare la corrispondente serie di potenze formali. Tale strumento non è cosí potente come nel caso olomorfo, ma può essere molto utile. Il processo mediante il quale si sostituiscono i polinomi con le serie di potenze formali è un esempio di una costruzione di carattere generale, nota come *completamento*. Un altro esempio importante di completamento si presenta in teoria dei numeri nella formazione dei numeri p-adici. Se p è un numero primo in $\mathbf{Z}$ si può lavorare nei vari anelli quozienti $\mathbf{Z}/p^n\mathbf{Z}$: in altre parole, si può tentare di risolvere le congruenze modulo p^n per valori sempre piú grandi di n. Ciò è analogo alle approssimazioni successive date dai termini di uno sviluppo in serie di Taylor e, proprio com'è conveniente introdurre le serie di potenze formali, cosí è conveniente introdurre i numeri p-adici, i quali sono, in un certo senso, il limite di $\mathbf{Z}/p^n\mathbf{Z}$ per $n \to \infty$. Per un solo aspetto, tuttavia, i numeri p-adici sono piú complicati rispetto alle serie di potenze formali (diciamo, in una variabile x). Mentre i polinomi di grado n si immergono, in modo naturale, nelle serie di potenze, il gruppo $\mathbf{Z}/p^n\mathbf{Z}$ non può essere immerso nell'anello completato $\hat{\mathbf{Z}}$. Sebbene un intero p-adico possa essere pensato come una serie di potenze $\sum a_n p^n$ $(0 \leqslant a_n < p)$, tale rappresentazione non si comporta bene rispetto alle operazioni di un anello.

In questo capitolo descriveremo il processo generale di completamento "adico"— dove il numero primo p è sostituito da un ideale arbitrario. Tale processo si esprime molto agevolmente in termini topologici, ma il lettore dovrebbe guardarsi dall'usare la topologia dei numeri reali come guida per l'intuizione. Egli dovrebbe pensare invece alla topologia delle serie di potenze in cui una serie di potenze è "piccola" se possiede soltanto termini di grado elevato. Oppure egli può pensare alla topologia p-adica su Z, in cui un intero è "piccolo" se è divisibile per una potenza elevata di p.

Il completamento, al pari della localizzazione, è un metodo che permette di semplificare le cose, concentrando l'attenzione nell'intorno di un punto (o di un ideale primo). Esso costituisce tuttavia una semplificazione più drastica rispetto alla localizzazione. Per esempio, in geometria algebrica, l'anello locale di un punto non singolare su una varietà di dimensione n ha sempre, come suo completamento, l'anello delle serie di potenze formali in n variabili (ciò sarà sostanzialmente dimostrato nel Capitolo 11). D'altra parte, gli anelli locali di due punti siffatti non possono essere isomorfi a meno che le varietà su cui essi si trovano non sono birazionalmente equivalenti (ciò significa che i campi delle frazioni dei due anelli locali sono isomorfi).

Due proprietà importanti della localizzazione sono date dal fatto che essa conserva l'esattezza e la noetherianità. Ciò vale anche per il completamento — quando ci si restringe ai moduli finitamente generati — ma le dimostrazioni sono molto più difficili e assorbono la maggior parte del capitolo. Un altro risultato importante è il teorema di Krull che precisa la parte di un anello che "svanisce" nel completamento. In breve, il teorema di Krull è l'analogo del fatto che una funzione analitica è individuata dai coefficienti del suo sviluppo in serie di Taylor. Tale analogia è molto più chiara per un anello locale noetheriano, nel qual caso il teorema asserisce proprio che $\bigcap \mathfrak{m}^n = 0$, dove $\mathfrak{m}$ è l'ideale massimale. Sia il teorema di Krull che l'esattezza del completamento sono facili conseguenze del ben noto "lemma di Artin-Rees", e a tale lemma viene assegnato un posto centrale nella nostra trattazione.

Per lo studio dei completamenti sarà necessario introdurre gli anelli graduati. Il prototipo di anello graduato è l'anello dei polinomi $k[x_1, \ldots, x_n]$, dove la graduazione è quella usuale, ottenuta assegnando a ciascuna variabile grado 1. Così come gli anelli non graduati sono la base della geometria algebrica affine, allo stesso modo gli anelli graduati sono la base della geometria algebrica proiettiva. Essi sono pertanto di notevole interesse geometrico. L'importante costruzione dell'anello graduato associato $G_\mathfrak{a}(A)$ di un ideale $\mathfrak{a}$ di A, che incontreremo, possiede una ben definita interpretazione geometrica. Per esempio, se A è l'anello locale di un punto P su una varietà V con ideale massimale $\mathfrak{a}$, allora $G_\mathfrak{a}(A)$ corrisponde al cono tangente proiettivizzato in P, ossia, all'insieme di tutte le rette per P che sono tangenti a

V in P. Tale descrizione geometrica dovrebbe aiutare a spiegare il significato di $G_0(A)$ in relazione alle proprietà di V nell'intorno di P e in particolare in relazione allo studio dell'anello completato $\hat{A}$.

Topologie e completamenti

Sia G un gruppo abeliano topologico (scritto in forma additiva), non necessariamente di Hausdorff: dunque G è simultaneamente uno spazio topologico ed un gruppo abeliano, e le due strutture su G sono compatibili nel senso che le applicazioni $G \times G \to G$ e $G \to G$, definite da $(x, y) \mapsto x + y$ e $x \mapsto -x$ rispettivamente, sono continue. Se $\{0\}$ è chiuso in G, allora l'insieme diagonale è chiuso in $G \times G$ (essendo l'immagine inversa di $\{0\}$ nell'applicazione $(x, y) \mapsto x - y$) e quindi G è uno spazio di Hausdorff. Se a è un elemento fissato di G, la traslazione T_a definita ponendo $T_a(x) = x + a$ è un omeomorfismo di G sopra G (giacché T_a è continua, e la sua inversa è T_{-a}); ne segue che se U è un intorno arbitrario di 0 in G, allora $U + a$ è un intorno di a in G, e viceversa ogni intorno di a compare in questa forma. Dunque la topologia di G è determinata univocamente dagli intorni di 0 in G.

Lemma 10.1. *Sia H l'intersezione di tutti gli intorni di 0 in G. Allora:*

i) *H è un sottogruppo.*
ii) *H è la chiusura di $\{0\}$.*
iii) *G/H è di Hausdorff.*
iv) *G è di Hausdorff $\Leftrightarrow H = 0$.*

Dimostrazione. i) segue dalla continuità delle operazioni di gruppo. Per ii) si ha:

$$x \in H \Leftrightarrow 0 \in x - U \text{ per ogni intorno } U \text{ di } 0 \Leftrightarrow x \in \overline{\{0\}}.$$

ii) implica che tutte le classi laterali di H sono sottoinsiemi chiusi; pertanto i punti sono chiusi in G/H e quindi G/H è di Hausdorff. Dunque $H = 0 \Rightarrow G$ è di Hausdorff, e il viceversa è banale. ∎

Supponiamo per semplicità che $0 \in G$ possiede un sistema fondamentale numerabile di intorni. Allora il completamento $\hat{G}$ di G può essere definito nel modo usuale, mediante le successioni di Cauchy. Si definisce *successione di Cauchy* in G una successione (x_ν) di elementi di G tale che, per ogni intorno U di 0, esiste un intero $s(U)$ con la proprietà che

$$x_\mu - x_\nu \in U \text{ per ogni } \mu, \nu \geqslant s(U).$$

Due successioni di Cauchy sono *equivalenti* se $x_\nu - y_\nu \to 0$ in G. L'insieme di tutte le classi di equivalenza di successioni di Cauchy si denota con $\hat{G}$. Se (x_ν), (y_ν) sono successioni di Cauchy, tale risulta $(x_\nu + y_\nu)$, e la sua classe in $\hat{G}$ dipende soltanto dalle classi di (x_ν) e (y_ν). Dunque resta definita un'addizione in $\hat{G}$, rispetto alla quale $\hat{G}$ è un gruppo abeliano. Per ogni elemento $x \in G$, la classe della successione costante (x) è un elemento $\phi(x)$ di $\hat{G}$, e $\phi\colon G \to \hat{G}$ è un omomorfismo di gruppi abeliani. Conviene notare che in generale ϕ non è iniettivo. Infatti si ha

$$\operatorname{Ker} \phi = \bigcap U$$

dove U varia nell'insieme di tutti gli intorni di 0 in G, sicché, in virtú di (10.1), ϕ è iniettivo se e soltanto se G è di Hausdorff.

Se H è un altro gruppo abeliano topologico e $f\colon G \to H$ è un omomorfismo continuo, allora l'immagine mediante f di una successione di Cauchy in G è una successione di Cauchy in H, e pertanto f induce un omomorfismo $\hat{f}\colon \hat{G} \to \hat{H}$, il quale è continuo. Se si ha $G \xrightarrow{f} H \xrightarrow{g} K$, allora $\widehat{g \circ f} = \hat{g} \circ \hat{f}$.

Finora siamo rimasti in un ambito del tutto generale e G avrebbe potuto essere, per esempio, il gruppo additivo dei numeri razionali con la topologia usuale, cosicché $\hat{G}$ sarebbe stato l'insieme dei numeri reali. Ora, tuttavia, ci limitiamo a considerare il tipo particolare di topologia che si presenta in algebra commutativa, ossia supponiamo che $0 \in G$ abbia un sistema fondamentale di intorni costituito da *sottogruppi*. Si ha così una successione di sottogruppi

$$G = G_0 \supseteq G_1 \supseteq \quad \supseteq G_n \supseteq$$

e $U \subseteq G$ è un intorno di 0 se e soltanto se contiene qualche G_n. Un tipico esempio è la topologia p-adica su $\mathbf{Z}$, in cui $G_n = p^n\mathbf{Z}$. Si noti che in tali topologie i sottogruppi G_n di G sono simultaneamente aperti e chiusi. Infatti, se $g \in G_n$, allora $g + G_n$ è un intorno di g; poiché $g + G_n \subseteq G_n$, ciò mostra che G_n è aperto. Dunque per ogni h la classe laterale $h + G_n$ è un aperto e pertanto l'insieme $\bigcup_{h \notin G_n} (h + G_n)$ è aperto; poiché tale insieme è il complementare di G_n in G, ne segue che G_n è chiuso.

Per le topologie definite da successioni di sottogruppi vi è una definizione alternativa puramente algebrica del completamento, la quale spesso è comoda. Supponiamo che (x_ν) sia una successione di Cauchy in G. Allora l'immagine di x_ν in G/G_n è costante, da un certo punto in poi, ed è uguale, diciamo, a ξ_n. Se si passa da $n+1$ a n è chiaro che si ha $\xi_{n+1} \mapsto \xi_n$ mediante la proiezione

$$G/G_{n+1} \xrightarrow{\theta_{n+1}} G/G_n.$$

Dunque una successione di Cauchy (x_ν) in G definisce una *successione coerente* (ξ_n) nel senso che

$$\theta_{n+1}(\xi_{n+1}) = \xi_n \text{ per ogni } n.$$

Inoltre è chiaro che successioni di Cauchy equivalenti definiscono una medesima successione (ξ_n). Infine, data una qualsiasi successione coerente (ξ_n), si può costruire una successione di Cauchy (x_n), essendo x_n un elemento arbitrariamente scelto nella classe ξ_n (cosicché $x_{n+1} - x_n \in G_n$). Dunque $\hat{G}$ può essere definito anche come l'insieme delle successioni coerenti (ξ_n) con la struttura naturale di gruppo.

Siamo pervenuti ora ad un caso particolare di *limite inverso*. Più in generale, consideriamo un'arbitraria successione di gruppi $\{A_n\}$ e di omomorfismi

$$\theta_{n+1}: A_{n+1} \to A_n.$$

Tale successione prende il nome di *sistema inverso*, e il gruppo di tutte le successioni coerenti (a_n) (ossia, $a_n \in A_n$ e $\theta_{n+1}(a_{n+1}) = a_n$) è chiamato il *limite inverso* del sistema. Esso viene indicato di solito con $\varprojlim A_n$, essendo sottintesi gli omomorfismi θ_n. Con tale notazione si ha

$$\hat{G} \cong \varprojlim G/G_n.$$

La definizione di $\hat{G}$ come limite inverso presenta molti vantaggi. Il suo principale inconveniente è che essa presuppone una scelta fissata dei sottogruppi G_n. Ora può accadere che successioni distinte di G_n definiscono la medesima topologia e quindi il medesimo completamento. Naturalmente si potrebbe definire la nozione di sistemi inversi "equivalenti", ma il vantaggio del linguaggio topologico è precisamente quello che tali nozioni sono già incorporate in esso.

Le proprietà di esattezza del completamento si studiano meglio mediante i limiti inversi. Osserviamo innanzitutto che il sistema inverso G/G_n ha la particolare proprietà che θ_{n+1} è sempre suriettivo. Un sistema inverso con tale proprietà prende il nome di sistema *su-*

riettivo. Supponiamo ora che $\{A_n\}$, $\{B_n\}$, $\{C_n\}$ siano tre sistemi inversi e che si abbiano diagrammi commutativi di successioni esatte

$$\begin{array}{ccccccccc} 0 & \to & A_{n+1} & \to & B_{n+1} & \to & C_{n+1} & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & A_n & \longrightarrow & B_n & \longrightarrow & C_n & \longrightarrow & 0. \end{array}$$

Diremo allora che si ha una successione esatta di sistemi inversi. Il diagramma induce certamente degli omomorfismi

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$$

ma tale successione *non* è sempre esatta. Vale tuttavia la

Proposizione 10.2. *Se* $0 \to \{A_n\} \to \{B_n\} \to \{C_n\} \to 0$ *è una successione esatta di sistemi inversi, allora*

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n$$

è sempre esatta. Se, inoltre, $\{A_n\}$ *è un sistema suriettivo, allora*

$$0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$$

è esatta.

Dimostrazione. Poniamo $A = \prod_{n=1}^{\infty} A_n$ e definiamo $d^A \colon A \to A$ ponendo $d^A(a_n) = a_n - \theta_{n+1}(a_{n+1})$. Allora $\operatorname{Ker} d^A \cong \varprojlim A_n$. Allo stesso modo definiamo B, C e d^B, d^C. La successione esatta di sistemi inversi definisce allora un diagramma commutativo di successioni esatte

$$\begin{array}{ccccccccc} 0 & \to & A & \to & B & \to & C & \to & 0 \\ & & \downarrow{\scriptstyle d^A} & & \downarrow{\scriptstyle d^B} & & \downarrow{\scriptstyle d^C} & & \\ 0 & \to & A & \to & B & \to & C & \to & 0 \end{array}$$

e quindi, in virtú di (2.10), una successione esatta

$$\begin{aligned} 0 \to \operatorname{Ker} d^A \to \operatorname{Ker} d^B \to \operatorname{Ker} d^C \to \\ \to \operatorname{Coker} d^A \to \operatorname{Coker} d^B \to \operatorname{Coker} d^C \to 0. \end{aligned}$$

Per completare la dimostrazione occorre provare soltanto che

$$\{A_n\} \text{ suriettivo} \Rightarrow d^A \text{ suriettivo},$$

ma ciò è chiaro, poiché per dimostrare che d^A è suriettivo c'è soltanto da risolvere induttivamente le equazioni

$$x_n - \theta_{n+1}(x_{n+1}) = a_n$$

per $x_n \in A_n$, assegnati gli elementi $a_n \in A_n$. ■

Osservazione. Il gruppo Coker d^A viene denotato di solito con $\varprojlim^1 A_n$, poiché è un funtore derivato nel senso dell'algebra omologica.

Corollario 10.3. *Sia* $0 \to G' \to G \xrightarrow{p} G'' \to 0$ *una successione esatta di gruppi. Supponiamo che* G *abbia la topologia definita da una successione* $\{G_n\}$ *di sottogruppi, e* G', G'' *abbiano le topologie indotte, ossia, le topologie definite dalle successioni* $\{G' \cap G_n\}$, $\{p(G_n)\}$. *Allora*

$$0 \to \hat{G}' \to \hat{G} \to \hat{G}'' \to 0$$

è esatta.

Dimostrazione. Basta applicare (10.2) alle successioni esatte

$$0 \to \frac{G'}{G' \cap G_n} \to \frac{G}{G_n} \to \frac{G''}{p(G_n)} \to 0. \quad ■$$

In particolare, possiamo applicare (10.3) con $G' = G_n$; allora $G'' = G/G_n$ ha la topologia discreta, cosicché $\hat{G}'' = G''$. Da ciò si deduce il

Corollario 10.4. $\hat{G}_n$ *è un sottogruppo di* $\hat{G}$ *e*

$$\hat{G}/\hat{G}_n \cong G/G_n. \quad ■$$

Prendendo i limiti inversi in (10.4) si ottiene:

Proposizione 10.5. $\hat{\hat{G}} \cong \hat{G}$. ■

Se $\phi\colon G \to \hat{G}$ è un isomorfismo, diremo che G è *completo*. Dunque (10.5) afferma che il completamento di G è completo. Occorre notare che la nostra definizione di completezza include la proprietà di Hausdorff (in virtù di (10.1)).

La classe più importante di esempi di gruppi topologici del tipo che stiamo considerando si ottiene prendendo $G = A$, $G_n = \mathfrak{a}^n$, dove $\mathfrak{a}$ è un ideale in un anello A. La topologia cosí definita su A prende il nome di *topologia* $\mathfrak{a}$*-adica*, o semplicemente, di $\mathfrak{a}$*-topologia*. Poiché gli $\mathfrak{a}^n$ sono ideali, non è difficile verificare che con tale topologia A risulta un *anello topologico*, ossia le operazioni di anello sono continue. In virtú di (10.1) la topologia è di Hausdorff $\Leftrightarrow \bigcap \mathfrak{a}^n = (0)$. Il *completamento* $\hat{A}$ di A è ancora un anello topologico; $\phi: A \to \hat{A}$ è un omomorfismo continuo di anelli, il cui nucleo è $\bigcap \mathfrak{a}^n$.

Similmente si procede per un A-modulo M: si prende $G = M$, $G_n = \mathfrak{a}^n M$. Ciò definisce la $\mathfrak{a}$*-topologia* su M, e il completamento $\hat{M}$ di M è un $\hat{A}$-modulo topologico (ossia $\hat{A} \times \hat{M} \to \hat{M}$ è continua). Se $f: M \to N$ è un arbitrario omomorfismo di A-moduli, allora $f(\mathfrak{a}^n M) = \mathfrak{a}^n f(M) \subseteq \mathfrak{a}^n N$, e pertanto f è continuo (rispetto alle $\mathfrak{a}$-topologie su M e N) e quindi definisce un omomorfismo $\hat{f}: \hat{M} \to \hat{N}$.

Esempi. 1) $A = k[x]$, dove k è un campo e x è un'indeterminata; $\mathfrak{a} = (x)$. Allora $\hat{A} = k[[x]]$, l'anello delle serie di potenze formali.

2) $A = \mathbf{Z}$, $\mathfrak{a} = (p)$, con p primo. Allora $\hat{A}$ è l'anello degli *interi* p*-adici*. I suoi elementi sono le serie infinite $\sum_{n=0}^{\infty} a_n p^n$, con $0 \leqslant a_n \leqslant p-1$. Si ha $p^n \to 0$ per $n \to \infty$.

Filtrazioni

La $\mathfrak{a}$-topologia di un A-modulo M è stata definita prendendo i sottomoduli $\mathfrak{a}^n M$ come intorni fondamentali di 0, ma vi sono altri modi di definire la medesima topologia. Una catena (infinita) $M = M_0 \supseteq M_1 \supseteq \ldots \supseteq M_n \supseteq \ldots$, dove gli M_n sono *sottomoduli* di M, è chiamata una *filtrazione* di M, e si denota con (M_n). Si dice che essa è una $\mathfrak{a}$*-filtrazione*, se $\mathfrak{a} M_n \subseteq M_{n+1}$ per ogni n, e una $\mathfrak{a}$*-filtrazione stabile*, se $\mathfrak{a} M_n = M_{n+1}$ per ogni n abbastanza grande. Dunque $(\mathfrak{a}^n M)$ è una $\mathfrak{a}$-filtrazione stabile.

Lemma 10.6. *Se (M_n), (M'_n) sono $\mathfrak{a}$-filtrazioni stabili di M, allora esse hanno differenze limitate: ossia, esiste un intero n_0 tale che $M_{n+n_0} \subseteq M'_n$ e $M'_{n+n_0} \subseteq M_n$ per ogni $n \geqslant 0$. Dunque tutte le $\mathfrak{a}$-filtrazioni stabili individuano una medesima topologia su M, precisamente la $\mathfrak{a}$-topologia.*

Dimostrazione. Basta prendere $M'_n = \mathfrak{a}^n M$. Poiché $\mathfrak{a} M_n \subseteq M_{n+1}$ per ogni n, si ha $\mathfrak{a}^n M \subseteq M_n$; inoltre $\mathfrak{a} M_n = M_{n+1}$ per ogni $n \geqslant n_0$, diciamo, sicché $M_{n+n_0} = \mathfrak{a}^n M_{n_0} \subseteq \mathfrak{a}^n M$. ∎

Anelli e moduli graduati

Un *anello graduato* è un anello A insieme con una famiglia $(A_n)_{n \geq 0}$ di sottogruppi del gruppo additivo di A, tale che $A = \bigoplus_{n=0}^{\infty} A_n$ e $A_m A_n \subseteq A_{m+n}$ per ogni $m, n \geq 0$. In tal modo A_0 è un subanello di A e ciascun A_n è un A_0-modulo.

Esempio. $A = k[x_1, \ldots, x_r]$, $A_n =$ insieme di tutti i polinomi omogenei di grado n.

Se A è un anello graduato, un *A-modulo graduato* è un A-modulo M insieme con una famiglia $(M_n)_{n \geq 0}$ di sottogruppi di M tali che $M = \bigoplus_{n=0}^{\infty} M_n$ e $A_m M_n \subseteq M_{m+n}$ per ogni $m, n \geq 0$. In tal modo ciascun M_n è un A_0-modulo. Un elemento x di M si dice *omogeneo*, se $x \in M_n$ per qualche n ($n =$ *grado* di x). Ogni elemento $y \in M$ può essere scritto in modo unico come una somma del tipo $\sum_n y_n$, dove $y_n \in M_n$ per ogni $n \geq 0$, e gli y_n sono tutti nulli, tranne al più un numero finito di essi. Le componenti non nulle y_n sono chiamate le *componenti omogenee* di y.

Se M, N sono A-moduli graduati, un *omomorfismo di A-moduli graduati* è un omomorfismo di A-moduli $f: M \to N$ tale che $f(M_n) \subseteq N_n$ per ogni $n \geq 0$.

Se A è un anello graduato, poniamo $A_+ = \bigoplus_{n>0} A_n$. A_+ è un ideale di A.

Proposizione 10.7. *Le seguenti condizioni sono equivalenti, per un anello graduato A:*

i) *A è un anello noetheriano;*

ii) *A_0 è noetheriano e A è una A_0-algebra finitamente generata.*

Dimostrazione. i) $\Rightarrow$ ii). $A_0 \cong A/A_+$, quindi è noetheriano. A_+ è un ideale di A, dunque è finitamente generato, diciamo da $x_1, \ldots, x_s$, che possiamo supporre elementi omogenei di A, di gradi $k_1, \ldots, k_s$ rispettivamente (tutti > 0). Sia A' il subanello di A generato da $x_1, \ldots, x_s$ sopra A_0. Proveremo che $A_n \subseteq A'$ per ogni $n \geq 0$, procedendo per induzione su n. Ciò è certamente vero per $n = 0$. Supponiamo $n > 0$ e sia $y \in A_n$. Poiché $y \in A_+$, y è una combinazione lineare degli x_i, diciamo $y = \sum_{i=1}^{s} a_i x_i$, dove $a_i \in A_{n-k_i}$ (per convenzione, $A_m = 0$ se $m < 0$). Poiché ciascun intero k_i è > 0, in virtú dell'ipotesi induttiva ciascun a_i risulta un polinomio negli x a coefficienti in A_0. Dunque tale risulta anche y, e pertanto $y \in A'$. Ne segue che $A_n \subseteq A'$ e quindi $A = A'$.

ii) $\Rightarrow$ i) in virtú del teorema della base di Hilbert (7.7). ∎

Sia A un anello (non graduato), $\mathfrak{a}$ un ideale di A. Allora si può costruire un anello graduato $A^* = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$. Similmente, se M è un A-modulo e (M_n) è una $\mathfrak{a}$-filtrazione di M, allora $M^* = \bigoplus_n M_n$ è un A^*-modulo graduato, poiché $\mathfrak{a}^m M_n \subseteq M_{m+n}$.

Se A è noetheriano, $\mathfrak{a}$ è finitamente generato, diciamo da $x_1, \ldots, x_r$; allora $A^* = A[x_1, \ldots, x_r]$ ed è noetheriano in virtú di (7.7).

Lemma 10.8. *Sia A un anello noetheriano, M un A-modulo finitamente generato, (M_n) una $\mathfrak{a}$-filtrazione di M. Allora le seguenti condizioni sono equivalenti:*

i) *M^* è un A^*-modulo finitamente generato;*

ii) *La filtrazione (M_n) è stabile.*

Dimostrazione. Ciascun M_n è finitamente generato, dunque tale risulta ciascun $Q_n = \bigoplus_{r=0}^{n} M_r$: esso è un *sottogruppo* di M^*, ma non (in generale) un *A^*-sottomodulo*. Tuttavia, esso ne genera uno, precisamente

$$M_n^* = M_0 \oplus \ldots \oplus M_n \oplus \mathfrak{a}M_n \oplus \mathfrak{a}^2 M_n \oplus \qquad \oplus \mathfrak{a}^r M_n \oplus$$

Poiché Q_n è finitamente generato come A-modulo, M_n^* è finitamente generato come A^*-modulo. Gli M_n^* formano una catena ascendente, la cui unione è M^*. Poiché A^* è noetheriano, M^* è finitamente generato come A^*-modulo $\Leftrightarrow$ la catena è stazionaria, ossia, $M^* = M_{n_0}^*$ per qualche $n_0 \Leftrightarrow M_{n_0+r} = \mathfrak{a}^r M_{n_0}$ per ogni $r \geqslant 0 \Leftrightarrow$ la filtrazione è stabile. ∎

Proposizione 10.9. (lemma di Artin-Rees). *Sia A un anello noetheriano, $\mathfrak{a}$ un ideale di A, M un A-modulo finitamente generato, (M_n) una $\mathfrak{a}$-filtrazione stabile di M. Se M' è un sottomodulo di M, allora $(M' \cap M_n)$ è una $\mathfrak{a}$-filtrazione stabile di M'.*

Dimostrazione. Si ha $\mathfrak{a}(M' \cap M_n) \subseteq \mathfrak{a}M' \cap \mathfrak{a}M_n \subseteq M' \cap M_{n+1}$, sicché $(M' \cap M_n)$ è una $\mathfrak{a}$-filtrazione. Dunque essa definisce un A^*-

modulo graduato, il quale è un sottomodulo di M^* e pertanto è finitamente generato (giacché A^* è noetheriano). A questo punto basta utilizzare (10.8). ■

Prendendo $M_n = \mathfrak{a}^n M$ si ottiene l'enunciato che comunemente è noto come il lemma di Artin-Rees:

Corollario 10.10. *Esiste un intero k tale che*

$$(\mathfrak{a}^n M) \cap M' = \mathfrak{a}^{n-k}((\mathfrak{a}^k M) \cap M')$$

per ogni $n \geqslant k$. ■

D'altra parte, combinando (10.9) con il lemma elementare (10.6) si ottiene la versione realmente significativa:

Teorema 10.11. *Sia A un anello noetheriano, $\mathfrak{a}$ un ideale, M un A-modulo finitamente generato e M' un sottomodulo di M. Allora le filtrazioni $\mathfrak{a}^n M'$ e $(\mathfrak{a}^n M) \cap M'$ hanno differenze limitate. In particolare, la $\mathfrak{a}$-topologia di M' coincide con la topologia indotta dalla $\mathfrak{a}$-topologia di M.* ■

Osservazione. In questo capitolo applicheremo l'ultima parte di (10.11) riguardante le topologie. Tuttavia, nel prossimo capitolo, avremo bisogno del risultato piú forte relativo alle differenze limitate.

Come prima applicazione di (10.11), combiniamo tale risultato insieme con (10.3) in modo da ottenere l'importante *proprietà di esattezza del completamento*:

Proposizione 10.12. *Sia*

$$0 \to M' \to M \to M'' \to 0$$

una successione esatta di moduli finitamente generati sopra un anello noetheriano A. Sia $\mathfrak{a}$ un ideale di A, allora la successione dei completamenti $\mathfrak{a}$-adici

$$0 \to \hat{M}' \to \hat{M} \to \hat{M}'' \to 0$$

è esatta. ■

Poiché si ha un omomorfismo naturale $A \to \hat{A}$, si può riguardare $\hat{A}$ come una A-algebra e quindi per ogni A-modulo M si può costruire un $\hat{A}$-modulo $\hat{A} \otimes_A M$. È naturale chiedersi quali legami esistono tra tale modulo e l'$\hat{A}$-modulo $\hat{M}$. Ebbene l'omomorfismo di

A-moduli $M \to \hat{M}$ definisce un omomorfismo di $\hat{A}$-moduli

$$\hat{A} \otimes_A M \to \hat{A} \otimes_A \hat{M} \to \hat{A} \otimes_{\hat{A}} \hat{M} = \hat{M}.$$

In generale, per una scelta arbitraria di A e M, tale omomorfismo non è né iniettivo, né suriettivo; vale tuttavia la

Proposizione 10.13. *Per un anello arbitrario A, se M è finitamente generato, $\hat{A} \otimes_A M \to \hat{M}$ è suriettivo. Se inoltre, A è noetheriano, allora $\hat{A} \otimes_A M \to \hat{M}$ è un isomorfismo.*

Dimostrazione. Utilizzando (10.3) o procedendo per altra via, è chiaro che il completamento $\mathfrak{a}$-adico commuta con le somme dirette finite. Dunque, se $F \cong A^n$ si ha $\hat{A} \otimes_A F \cong \hat{F}$. Supponiamo ora che M sia finitamente generato, sicché si ha una successione esatta

$$0 \to N \to F \to M \to 0.$$

Essa dà origine al diagramma commutativo

$$\begin{tikzcd}
& \hat{A} \otimes_A N \arrow[r] \arrow[d, "\gamma"] & \hat{A} \otimes_A F \arrow[r] \arrow[d, "\beta"] & \hat{A} \otimes_A M \arrow[r] \arrow[d, "\alpha"] & 0 \\
0 \arrow[r] & \hat{N} \arrow[r] & \hat{F} \arrow[r, "\delta"] & \hat{M} \arrow[r] & 0
\end{tikzcd}$$

in cui la prima riga è esatta (stante (2.18)). In virtú di (10.3), δ è suriettivo. Poiché β è un isomorfismo, ciò implica che α è suriettivo, sicché resta provata la prima parte della proposizione. Supponiamo ora che A sia noetheriano, allora anche N è finitamente generato, sicché γ è suriettivo e, in virtú di (10.12), la riga inferiore è esatta. Una piccola "caccia al diagramma" mostra ora che α è iniettivo e quindi è un isomorfismo. ∎

Le proposizioni (10.12) e (10.13) insieme affermano che il funtore $M \mapsto \hat{A} \otimes_A M$ è esatto sulla categoria degli A-moduli finitamente generati (quando A è noetheriano). Come si è visto nel Capitolo 2, ciò prova:

Proposizione 10.14. *Se A è un anello noetheriano, $\mathfrak{a}$ un ideale, $\hat{A}$ il completamento $\mathfrak{a}$-adico di A, allora $\hat{A}$ è una A-algebra piatta.* ∎

Osservazione. Per i moduli non finitamente generati il funtore $M \mapsto \hat{M}$ non è esatto: il funtore "buono", che è esatto, è $M \mapsto \hat{A} \otimes_A M$ e i due funtori coincidono sui moduli finitamente generati.

Passiamo ora a studiare piú dettagliatamente l'anello $\hat{A}$. Dimostriamo innanzitutto alcune proposizioni elementari:

Proposizione 10.15. *Se A è noetheriano, $\hat{A}$ il suo completamento $\mathfrak{a}$-adico, allora:*

i) $\hat{\mathfrak{a}} = \hat{A}\mathfrak{a} \cong \hat{A} \otimes_A \mathfrak{a}$;

ii) $(\mathfrak{a}^n)^\wedge = (\hat{\mathfrak{a}})^n$;

iii) $\mathfrak{a}^n/\mathfrak{a}^{n+1} \cong \hat{\mathfrak{a}}^n/\hat{\mathfrak{a}}^{n+1}$;

iv) $\hat{\mathfrak{a}}$ *è contenuto nel radicale di Jacobson di* $\hat{A}$.

Dimostrazione. Poiché A è noetheriano, $\mathfrak{a}$ è finitamente generato. Allora (10.13) implica che l'applicazione

$$\hat{A} \otimes_A \mathfrak{a} \to \hat{\mathfrak{a}},$$

la cui immagine è $\hat{A}\mathfrak{a}$, è un isomorfismo. Ciò dimostra i). Applicando i) ad $\mathfrak{a}^n$ si ottiene

$$\begin{aligned} (\mathfrak{a}^n)^\wedge = \hat{A}\mathfrak{a}^n &= (\hat{A}\mathfrak{a})^n && \text{in virtú di (1.18)} \\ &= (\hat{\mathfrak{a}})^n && \text{stante i).} \end{aligned}$$

Applicando (10.4) si deduce ora

$$A/\mathfrak{a}^n \cong \hat{A}/\hat{\mathfrak{a}}^n$$

da cui segue iii), passando ai quozienti. In virtú di ii) e di (10.5) si ha che $\hat{A}$ è completo rispetto alla sua $\hat{\mathfrak{a}}$-topologia. Dunque per ogni $x \in \hat{\mathfrak{a}}$

$$(1 - x)^{-1} = 1 + x + x^2 +$$

converge in $\hat{A}$, sicché $1 - x$ è invertibile. Ciò implica, in virtú di (1.9), che $\hat{\mathfrak{a}}$ è contenuto nel radicale di Jacobson di $\hat{A}$. ∎

Proposizione 10.16. *Sia A un anello locale noetheriano, $\mathfrak{m}$ il suo ideale massimale. Allora il completamento $\mathfrak{m}$-adico $\hat{A}$ di A è un anello locale con ideale massimale $\hat{\mathfrak{m}}$.*

Dimostrazione. In virtú di (10.15) iii), si ha $\hat{A}/\hat{\mathfrak{m}} \cong A/\mathfrak{m}$, sicché $\hat{A}/\hat{\mathfrak{m}}$ è un campo e quindi $\hat{\mathfrak{m}}$ è un ideale massimale. Da (10.15) iv) segue che $\hat{\mathfrak{m}}$ è il radicale di Jacobson di $\hat{A}$ e quindi è l'unico ideale massimale. Dunque $\hat{A}$ è un anello locale. ∎

Il problema importante di sapere quanto si perde nel completamento è risolto dal teorema di Krull:

Teorema 10.17. *Sia A un anello noetheriano, $\mathfrak{a}$ un ideale, M un A-modulo finitamente generato e $\hat{M}$ l'$\mathfrak{a}$-completamento di M. Allora il nucleo $E = \bigcap_{n=1}^{\infty} \mathfrak{a}^n M$ di $M \to \hat{M}$ è costituito dagli elementi $x \in M$ che sono annullati da qualche elemento di $1 + \mathfrak{a}$.*

Dimostrazione. Poiché E è l'intersezione di tutti gli intorni di $0 \in M$, la topologia indotta su E è banale, ossia, E è l'unico intorno di $0 \in E$. In virtú di (10.11) la topologia indotta su E coincide con la sua $\mathfrak{a}$-topologia. Essendo $\mathfrak{a}E$ un intorno nella $\mathfrak{a}$-topologia, ne segue che $\mathfrak{a}E = E$. Poiché M è finitamente generato e A è noetheriano, anche E è finitamente generato, sicché possiamo applicare (2.5) e dedurre da $\mathfrak{a}E = E$ che $(1 - \alpha)E = 0$ per qualche $\alpha \in \mathfrak{a}$. Il viceversa è ovvio: se $(1 - \alpha)x = 0$, allora

$$x = \alpha x = \alpha^2 x = \qquad \in \bigcap_{n=1}^{\infty} \mathfrak{a}^n M = E. \quad \blacksquare$$

Osservazioni. 1) Se S è la parte moltiplicativa $1 + \mathfrak{a}$, allora (10.17) asserisce che

$$A \to \hat{A} \text{ e } A \to S^{-1}A$$

hanno lo stesso nucleo. Inoltre, per ogni $\alpha \in \hat{\mathfrak{a}}$

$$(1 - \alpha)^{-1} = 1 + \alpha + \alpha^2 +$$

converge in $\hat{A}$, sicché ogni elemento di S diventa invertibile in $\hat{A}$. In virtú della proprietà universale di $S^{-1}A$, ciò significa che vi è un omomorfismo naturale $S^{-1}A \to \hat{A}$ e (10.17) implica che esso è iniettivo. Dunque $S^{-1}A$ può essere identificato con un subanello di $\hat{A}$.

2) Il teorema di Krull (10.17) può essere falso, se A non è noetheriano. Sia A l'anello di tutte le funzioni C^∞ sulla retta reale, e sia $\mathfrak{a}$ l'ideale di tutte le funzioni f che si annullano nell'origine ($\mathfrak{a}$ è massimale, giacché $A/\mathfrak{a} \cong \mathbf{R}$). Ora $\mathfrak{a}$ è generato dalla funzione identità x, e $\bigcap_{n=1}^{\infty} \mathfrak{a}^n$ è l'insieme di tutte le funzioni $f \in A$ tali che tutte le loro derivate si annullano nell'origine. D'altra parte f è annullata da qualche elemento $1 + \alpha$ ($\alpha \in \mathfrak{a}$) se e soltanto se f si annulla identicamente in qualche intorno di 0. La ben nota funzione e^{-1/x^2}, la quale non è identicamente nulla in alcun intorno di 0, ma è tale che tutte le sue derivate si annullano in 0, mostra allora che i nuclei di

$$A \to \hat{A} \text{ e } A \to S^{-1}A \qquad (S = 1 + \mathfrak{a})$$

non coincidono. Dunque A non è noetheriano.

Il teorema di Krull ha molti corollari:

Corollario 10.18. *Sia A un dominio noetheriano, $\mathfrak{a} \neq (1)$ un ideale di A. Allora $\bigcap \mathfrak{a}^n = 0$.*

Dimostrazione. $1 + \mathfrak{a}$ non contiene divisori dello zero. ∎

Corollario 10.19. *Sia A un anello noetheriano, $\mathfrak{a}$ un ideale di A contenuto nel radicale di Jacobson e sia M un A-modulo finitamente generato. Allora la $\mathfrak{a}$-topologia di M è di Hausdorff, ossia $\bigcap \mathfrak{a}^n M = 0$.*

Dimostrazione. In virtú di (1.9) ogni elemento di $1 + \mathfrak{a}$ è invertibile. ∎

Un caso speciale particolarmente importante di (10.19) è il seguente:

Corollario 10.20. *Sia A un anello locale noetheriano, $\mathfrak{m}$ il suo ideale massimale, M un A-modulo finitamente generato. Allora la $\mathfrak{m}$-topologia di M è di Hausdorff. In particolare la $\mathfrak{m}$-topologia di A è di Hausdorff.* ∎

È possibile rienunciare (10.20) in una forma leggermente diversa, ricordando che un ideale $\mathfrak{m}$-primario di A è proprio un ideale qualsiasi situato tra $\mathfrak{m}$ e qualche potenza $\mathfrak{m}^n$ (utilizzare (4.2) e (7.14)). Ebbene (10.20) implica che l'intersezione di tutti gli ideali $\mathfrak{m}$-primari di A è 0. Ora, se A è un anello noetheriano qualsiasi, e $\mathfrak{p}$ è un ideale primo, possiamo applicare tale versione di (10.20) all'anello locale $A_\mathfrak{p}$. Tornando indietro in A e utilizzando la corrispondenza biunivoca (4.8) tra gli ideali $\mathfrak{p}$-primari di A e gli ideali $\mathfrak{m}$-primari di $A_\mathfrak{p}$ (dove $\mathfrak{m} = \mathfrak{p}A_\mathfrak{p}$) si deduce:

Corollario 10.21. *Sia A un anello noetheriano, $\mathfrak{p}$ un ideale primo di A. Allora l'intersezione di tutti gli ideali $\mathfrak{p}$-primari di A è il nucleo dell'omomorfismo $A \to A_\mathfrak{p}$.* ∎

L'anello graduato associato

Sia A un anello e $\mathfrak{a}$ un ideale di A. Definiamo

$$G(A)\ (= G_\mathfrak{a}(A)) = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n/\mathfrak{a}^{n+1} \qquad (\mathfrak{a}^0 = A).$$

Si tratta di un anello graduato, in cui la moltiplicazione è definita nel modo seguente:

Per ogni $x_n \in \mathfrak{a}^n$, denotiamo con $\bar{x}_n$ l'immagine di x_n in $\mathfrak{a}^n/\mathfrak{a}^{n+1}$; definiamo $\bar{x}_m\bar{x}_n$ uguale a $\overline{x_m x_n}$, ossia all'immagine di $x_m x_n$ in $\mathfrak{a}^{m+n}/\mathfrak{a}^{m+n+1}$; si verifica che $\bar{x}_m\bar{x}_n$ non dipende dai rappresentanti scelti.

Similmente, se M è un A-modulo e (M_n) è una $\mathfrak{a}$-filtrazione di M, definiamo

$$G(M) = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}$$

il quale risulta, in modo naturale, un $G(A)$-modulo graduato. Denotiamo M_n/M_{n+1} con $G_n(M)$.

Proposizione 10.22. *Sia A un anello noetheriano, $\mathfrak{a}$ un ideale di A. Allora:*

i) *$G_\mathfrak{a}(A)$ è noetheriano;*

ii) *$G_\mathfrak{a}(A)$ e $G_{\hat{\mathfrak{a}}}(\hat{A})$ sono isomorfi come anelli graduati;*

iii) *se M è un A-modulo finitamente generato e (M_n) è una $\mathfrak{a}$-filtrazione stabile di M, allora $G(M)$ è un $G_\mathfrak{a}(A)$-modulo graduato finitamente generato.*

Dimostrazione. i) Poiché A è noetheriano, $\mathfrak{a}$ è finitamente generato, diciamo da $x_1, \ldots, x_r$. Sia $\bar{x}_i$ l'immagine di x_i in $\mathfrak{a}/\mathfrak{a}^2$, allora $G(A) = (A/\mathfrak{a})[\bar{x}_1, \ldots, \bar{x}_r]$. Ora $A/\mathfrak{a}$ è noetheriano, dunque $G(A)$ è noetheriano in virtú del teorema della base di Hilbert.

ii) $\mathfrak{a}^n/\mathfrak{a}^{n+1} \cong \hat{\mathfrak{a}}^n/\hat{\mathfrak{a}}^{n+1}$ in virtú di (10.15) iii).

iii) Esiste un intero n_0 tale che $M_{n_0+r} = \mathfrak{a}^r M_{n_0}$ per ogni $r \geqslant 0$, sicché $G(M)$ è generato da $\bigoplus_{n \leqslant n_0} G_n(M)$. Ciascun addendo $G_n(M) = M_n/M_{n+1}$ è noetheriano ed è annullato da $\mathfrak{a}$, dunque è un $A/\mathfrak{a}$-modulo finitamente generato; ne segue che $\bigoplus_{n \leqslant n_0} G_n(M)$ è generato da un numero finito di elementi (come $A/\mathfrak{a}$-modulo), e quindi $G(M)$ è finitamente generato come $G(A)$-modulo. ∎

L'ultimo risultato importante di questo capitolo è che il completamento $\mathfrak{a}$-adico di un anello noetheriano è noetheriano. Prima di passare alla dimostrazione, abbiamo bisogno di un semplice lemma che collega il completamento di un gruppo filtrato qualsiasi e il gruppo graduato associato.

Lemma 10.23. *Sia $\phi: A \to B$ un omomorfismo di gruppi filtrati, ossia $\phi(A_n) \subseteq B_n$, e siano $G(\phi): G(A) \to G(B)$, $\hat{\phi}: \hat{A} \to \hat{B}$ gli omomorfismi indotti dei gruppi graduati associati e dei gruppi completati. Allora*

i) *$G(\phi)$ iniettivo $\Rightarrow \hat{\phi}$ iniettivo;*

ii) *$G(\phi)$ suriettivo $\Rightarrow \hat{\phi}$ suriettivo.*

Dimostrazione. Consideriamo il diagramma commutativo di successioni esatte

$$\begin{array}{ccccccccc} 0 \to & A_n/A_{n+1} & \to & A/A_{n+1} & \to & A/A_n & \to 0 \\ & \downarrow{\scriptstyle G_n(\phi)} & & \downarrow{\scriptstyle \alpha_{n+1}} & & \downarrow{\scriptstyle \alpha_n} & \\ 0 \to & B_n/B_{n+1} & \to & B/B_{n+1} & \to & B/B_n & \to 0. \end{array}$$

Esso fornisce la successione esatta

$$\begin{aligned} 0 \to \operatorname{Ker} G_n(\phi) \to \operatorname{Ker} \alpha_{n+1} \to \operatorname{Ker} \alpha_n \to \\ \to \operatorname{Coker} G_n(\phi) \to \operatorname{Coker} \alpha_{n+1} \to \operatorname{Coker} \alpha_n \to 0. \end{aligned}$$

Da ciò si ottiene, per induzione su n, che $\operatorname{Ker} \alpha_n = 0$ (caso i)) oppure $\operatorname{Coker} \alpha_n = 0$ (caso ii)). Inoltre, nel caso ii) si ha anche che $\operatorname{Ker} \alpha_{n+1} \to \operatorname{Ker} \alpha_n$ è suriettivo. Prendendo il limite inverso degli omomorfismi α_n e applicando (10.2) si ottiene il lemma. ∎

Siamo ora in grado di stabilire un risultato che inverte parzialmente (10.22) iii) e costituisce il passo piú importante nella dimostrazione del fatto che $\hat{A}$ è noetheriano.

Proposizione 10.24. *Sia A un anello, $\mathfrak{a}$ un ideale di A, M un A-modulo, (M_n) una $\mathfrak{a}$-filtrazione di M. Supponiamo che A sia completo nella $\mathfrak{a}$-topologia e che M sia uno spazio di Hausdorff nella topologia definita dalla sua filtrazione (ossia che $\bigcap_n M_n = 0$). Supponiamo inoltre che $G(M)$ sia un $G(A)$-modulo finitamente generato. Allora M è un A-modulo finitamente generato.*

Dimostrazione. Scegliamo un sistema finito di generatori di $G(M)$ e decomponiamoli nelle loro componenti omogenee, diciamo $\xi_i (1 \leq i \leq r)$, dove ξ_i ha un certo grado $n(i)$, e pertanto è l'immagine di un qualche elemento $x_i \in M_{n(i)}$. Sia F^i il modulo A con la $\mathfrak{a}$-filtrazione stabile data da $F^i_k = \mathfrak{a}^{k+n(i)}$ e poniamo $F = \bigoplus_{i=1}^{r} F^i$. Allora mandando il generatore 1 di ciascun F^i in x_i, resta definito un omomorfismo

$$\phi \colon F \to M$$

di gruppi filtrati, e $G(\phi) \colon G(F) \to G(M)$ è un omomorfismo di $G(A)$-moduli. Per costruzione esso è suriettivo. Dunque, in virtú di

(10.23) ii), $\hat{\phi}$ è suriettivo. Consideriamo ora il diagramma

$$\begin{tikzcd} F \arrow[r, "\phi"] \arrow[d, "\alpha"'] & M \arrow[d, "\beta"] \\ \hat{F} \arrow[r, "\hat{\phi}"] & \hat{M} \end{tikzcd}$$

Poiché F è libero e $A = \hat{A}$, ne segue che α è un isomorfismo. Inoltre, essendo M uno spazio di Hausdorff, β è iniettivo. La suriettività di $\hat{\phi}$ implica dunque la suriettività di ϕ, e ciò significa che x_1, x_r generano M come A-modulo. ■

Corollario 10.25. *Nelle ipotesi di* (10.24), *se $G(M)$ è un $G(A)$-modulo noetheriano, allora M è un A-modulo noetheriano.*

Dimostrazione. Occorre provare che ogni sottomodulo M' di M è finitamente generato (6.2). Poniamo $M'_n = M' \cap M_n$; allora (M'_n) è una $\mathfrak{a}$-filtrazione di M', e l'immersione $M'_n \to M_n$ dà origine ad un omomorfismo iniettivo $M'_n/M'_{n+1} \to M_n/M_{n+1}$, dunque ad un'immersione di $G(M')$ in $G(M)$. Poiché $G(M)$ è noetheriano, $G(M')$ è finitamente generato, stante (6.2); inoltre M' è di Hausdorff, giacché $\bigcap M'_n \subseteq \bigcap M_n = 0$; dunque, in virtú di (10.24), M' è finitamente generato. ■

Siamo ora in grado di dedurre il risultato cercato:

Teorema 10.26. *Se A è un anello noetheriano, $\mathfrak{a}$ un ideale di A, allora il completamento $\mathfrak{a}$-adico $\hat{A}$ di A è noetheriano.*

Dimostrazione. Da (10.22) segue che

$$G_{\mathfrak{a}}(A) = G_{\hat{\mathfrak{a}}}(\hat{A})$$

è noetheriano. Applichiamo ora (10.25) all'anello completo $\hat{A}$, prendendo $M = \hat{A}$ (filtrato mediante $\hat{\mathfrak{a}}^n$, e quindi di Hausdorff). ■

Corollario 10.27. *Se A è un anello noetheriano, l'anello delle serie di potenze $B = A[[x_1, \ldots, x_n]]$ in n variabili è noetheriano. In particolare $k[[x_1, \ldots, x_n]]$ (essendo k un campo) è noetheriano.*

Dimostrazione. $A[x_1, \ldots, x_n]$ è noetheriano in virtú del teorema della base di Hilbert, e B è il suo completamento rispetto alla topologia $(x_1, \ldots, x_n)$-adica. ■

Esercizi

1. Sia $\alpha_n: \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p^n\mathbf{Z}$ l'omomorfismo iniettivo di gruppi abeliani definito ponendo $\alpha_n(1) = p^{n-1}$, e sia $\alpha: A \to B$ la somma diretta di tutti gli α_n (dove A è una somma diretta numerabile di copie di $\mathbf{Z}/p\mathbf{Z}$, e B è la somma diretta dei gruppi $\mathbf{Z}/p^n\mathbf{Z}$). Dimostrare che il completamento p-adico di A è proprio A, ma che il completamento di A rispetto alla topologia indotta dalla topologia p-adica su B è il *prodotto* diretto dei gruppi $\mathbf{Z}/p\mathbf{Z}$. Dedurre che il completamento p-adico *non* è un funtore esatto a destra sulla categoria di tutti gli $\mathbf{Z}$-moduli.

2. Nell'Esercizio 1, poniamo $A_n = \alpha^{-1}(p^nB)$, e consideriamo la successione esatta
$$0 \to A_n \to A \to A/A_n \to 0.$$
Dimostrare che $\varprojlim$ non è esatto a destra, e calcolare $\varprojlim^1 A_n$.

3. Sia A un anello noetheriano, $\mathfrak{a}$ un ideale e M un A-modulo finitamente generato. Utilizzando il teorema di Krull e l'Esercizio 14 del Capitolo 3, dimostrare che
$$\bigcap_{n=1}^{\infty} \mathfrak{a}^n M = \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \operatorname{Ker}(M \to M_{\mathfrak{m}}),$$
dove $\mathfrak{m}$ varia nell'insieme di tutti gli ideali massimali che contengono $\mathfrak{a}$.

   Dedurre che
$$\hat{M} = 0 \Leftrightarrow \operatorname{Supp}(M) \cap V(\mathfrak{a}) = \varnothing \quad (\text{in } \operatorname{Spec}(A)).$$
[Il lettore dovrebbe pensare a $\hat{M}$ come allo "sviluppo di Taylor" di M trasversalmente al "sottoschema" $V(\mathfrak{a})$: il risultato di cui sopra mostra allora che M è determinato in un intorno di $V(\mathfrak{a})$ dal suo sviluppo di Taylor.]

4. Sia A un anello noetheriano, $\mathfrak{a}$ un ideale in A, e $\hat{A}$ il completamento $\mathfrak{a}$-adico. Per ogni $x \in A$, sia $\hat{x}$ l'immagine di x in $\hat{A}$. Didal mostrare che
$$x \text{ non è un divisore dello zero in } A \Rightarrow$$
$$\Rightarrow \hat{x} \text{ non è un divisore dello zero in } \hat{A}.$$
Segue da ciò che
$$A \text{ è un dominio di integrità} \Rightarrow \hat{A} \text{ è un dominio di integrità?}$$

[Applicare la proprietà di esattezza del completamento alla successione $0 \to A \xrightarrow{x} A$.]

5. Sia A un anello noetheriano e siano $\mathfrak{a}, \mathfrak{b}$ ideali in A. Se M è un A-modulo arbitrario, denotiamo con $M^{\mathfrak{a}}, M^{\mathfrak{b}}$ il suo completamento $\mathfrak{a}$-adico, rispettivamente $\mathfrak{b}$-adico. Se M è finitamente generato, provare che $(M^{\mathfrak{a}})^{\mathfrak{b}} \cong M^{\mathfrak{a}+\mathfrak{b}}$.
[Prendere il completamento $\mathfrak{a}$-adico della successione esatta

$$0 \to \mathfrak{b}^m M \to M \to M/\mathfrak{b}^m M \to 0$$

e applicare (10.13). Utilizzare poi l'isomorfismo

$$\varprojlim_m (\varprojlim_n M/(\mathfrak{a}^n M + \mathfrak{b}^m M)) \cong \varprojlim_n M/(\mathfrak{a}^n M + \mathfrak{b}^n M)$$

e le inclusioni $(\mathfrak{a} + \mathfrak{b})^{2n} \subseteq \mathfrak{a}^n + \mathfrak{b}^n \subseteq (\mathfrak{a} + \mathfrak{b})^n$.]

6. Sia A un anello noetheriano e $\mathfrak{a}$ un ideale di A. Dimostrare che $\mathfrak{a}$ è contenuto nel radicale di Jacobson di A se e soltanto se ogni ideale massimale di A è chiuso rispetto alla $\mathfrak{a}$-topologia. (Un anello topologico noetheriano in cui la topologia è definita da un ideale contenuto nel radicale di Jacobson è chiamato un *anello di Zariski*. Esempi sono dati da anelli locali e (stante (10.15) (iv)) completamenti $\mathfrak{a}$-adici.)

7. Sia A un anello noetheriano, $\mathfrak{a}$ un ideale di A, e $\hat{A}$ il completamento $\mathfrak{a}$-adico. Dimostrare che $\hat{A}$ è fedelmente piatto sopra A (Capitolo 3, Esercizio 16) se e soltanto se A è un anello di Zariski (rispetto alla $\mathfrak{a}$-topologia).
[Poiché $\hat{A}$ è piatto sopra A, basta provare che

$M \to \hat{M}$ è iniettivo per ogni modulo finitamente generato M
$\Leftrightarrow A$ è di Zariski;

utilizzare poi (10.19) e l'Esercizio 6.]

8. Sia A l'anello locale dell'origine in $\mathbf{C}^n$ (ossia, l'anello di tutte le funzioni razionali $f/g \in \mathbf{C}(z_1, \ldots, z_n)$ con $g(0) \neq 0$), sia B l'anello delle serie di potenze in $z_1, \ldots, z_n$ che convergono in qualche intorno dell'origine, e sia C l'anello delle serie di potenze formali in $z_1, \ldots, z_n$, sicché $A \subset B \subset C$. Provare che B è un anello locale e che il suo completamento rispetto alla topologia definita dall'ideale massimale è C. Supponendo B noetheriano, dimostrare che B è piatto sopra A. [Utilizzare l'Esercizio 17 del Capitolo 3, e l'Esercizio 7 di cui sopra.]

9. Sia A un anello locale, $\mathfrak{m}$ il suo ideale massimale. Supponiamo che A sia completo rispetto alla topologia $\mathfrak{m}$-adica. Per ogni polinomio $f(x) \in A[x]$, denotiamo con $\bar{f}(x) \in (A/\mathfrak{m})[x]$ la sua riduzione mod $\mathfrak{m}$. Dimostrare il *lemma di Hensel*: se $f(x)$ è monico di grado n e se esistono polinomi monici coprimi $\bar{g}(x), \bar{h}(x) \in (A/\mathfrak{m})[x]$ di gradi $r, n-r$ con $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$, allora è possibile "sollevare" $\bar{g}(x), \bar{h}(x)$ in $A[x]$, in modo da ottenere polinomi monici $g(x), h(x) \in A[x]$ tali che $f(x) = g(x)h(x)$.
[Supponiamo di aver costruito induttivamente dei polinomi $g_k(x), h_k(x) \in A[x]$ tali che $g_k(x)h_k(x) - f(x) \in \mathfrak{m}^k A[x]$. Allora utilizziamo il fatto che, essendo $\bar{g}(x)$ e $\bar{h}(x)$ coprimi, è possibile trovare dei polinomi $\bar{a}_p(x), \bar{b}_p(x)$, di gradi $\leqslant n-r, r$ rispettivamente, tali che $x^p = \bar{a}_p(x)\bar{g}_k(x) + \bar{b}_p(x)\bar{h}_k(x)$, dove p è un intero qualsiasi tale che $1 \leqslant p \leqslant n$. Infine, utilizziamo la completezza di A per provare che le successioni $g_k(x), h_k(x)$ convergono verso i polinomi $g(x), h(x)$ cercati.]

10. i) Con le notazioni dell'Esercizio 9, dedurre dal lemma di Hensel che se $\bar{f}(x)$ possiede una radice semplice $\alpha \in A/\mathfrak{m}$, allora $f(x)$ possiede una radice semplice $a \in A$ tale che $\alpha = a$ mod $\mathfrak{m}$.
    ii) Dimostrare che 2 è un quadrato nell'anello degli interi 7-adici.
    iii) Sia $f(x, y) \in k[x, y]$, dove k è un campo, e supponiamo che $f(0, y)$ abbia $y = a_0$ come radice semplice. Provare che esiste una serie di potenze formale $y(x) = \sum_{n=0}^{\infty} a_n x^n$ tale che $f(x, y(x)) = 0$.
    (Essa rappresenta il "ramo analitico" della curva $f = 0$ per il punto $(0, a_0)$.)

11. Dimostrare che il viceversa di (10.26) è falso, anche supponendo che A sia locale e che $\hat{A}$ sia un A-modulo finitamente generato. [Prendere A uguale all'anello dei germi delle funzioni C^∞ di x in $x = 0$, e utilizzare il teorema di Borel secondo cui ogni serie di potenze è lo sviluppo di Taylor di qualche funzione C^∞.]

12. Se A è noetheriano, allora $A[[x_1, \ldots, x_n]]$ è una A-algebra fedelmente piatta. [Esprimere l'omomorfismo $A \to A[[x_1, \ldots, x_n]]$ come una composizione di estensioni piatte, e utilizzare l'Esercizio 5 (v) del Capitolo 1.]

Capitolo undicesimo

Teoria della dimensione

Una delle nozioni fondamentali in geometria algebrica è quella di dimensione di una varietà. Si tratta essenzialmente di una nozione locale, e, come vedremo in questo capitolo, vi è una teoria della dimensione molto soddisfacente per anelli locali noetheriani generali. Il teorema centrale stabilisce l'equivalenza di tre differenti definizioni di dimensione. Due di esse hanno un significato geometrico alquanto chiaro, mentre la terza, che fa intervenire la funzione di Hilbert, è meno concettuale. Questa tuttavia presenta molti vantaggi tecnici e l'intera teoria diventa piú agile se essa viene esaminata all'inizio.

Dopo aver trattato della dimensione, diamo alcuni brevi cenni sugli anelli locali regolari, i quali corrispondono alla nozione di non singolarità in geometria algebrica. Viene stabilita l'equivalenza di tre definizioni di regolarità.

Infine mostriamo come, nel caso di una varietà algebrica sopra un campo, le dimensioni locali da noi definite coincidono con il grado di trascendenza del campo di funzioni.

Funzioni di Hilbert

Sia $A = \bigoplus_{n=0}^{\infty} A_n$ un anello graduato noetheriano. In virtú di (10.7), A_0 è un anello noetheriano, e A è generato (come A_0-algebra) da elementi, diciamo $x_1, \ldots, x_s$, che possiamo supporre omogenei, di gradi $k_1, \ldots, k_s$ (tutti > 0).

Sia M un A-modulo graduato finitamente generato. Allora M è generato da un numero finito di elementi omogenei, diciamo m_j $(1 \leqslant j \leqslant t)$; poniamo $r_j = \deg m_j$. Ogni elemento di M_n, la componente omogenea di M di grado n, è dunque della forma $\sum_j f_j(x) m_j$, dove $f_j(x) \in A$ è un elemento omogeneo di grado $n - r_j$ (e pertanto è uguale a zero, se $n < r_j$). Ne segue che M_n è finitamente generato come A_0-modulo, precisamente, esso è generato da tutti gli elementi della forma $g_j(x)m_j$, dove $g_j(x)$ è un monomio negli x_i di grado totale $n - r_j$.

Sia λ una *funzione additiva* (a valori in $\mathbf{Z}$) sulla classe di tutti gli A_0-moduli finitamente generati (Capitolo 2). Si definisce *serie di Poincaré* di M (rispetto a λ) la funzione generatrice di $\lambda(M_n)$, ossia, la serie di potenze

$$P(M, t) = \sum_{n=0}^{\infty} \lambda(M_n)t^n \in \mathbf{Z}[[t]].$$

Teorema 11.1. (Hilbert, Serre). *$P(M, t)$ è una funzione razionale in t della forma $f(t)/\prod_{i=1}^{s}(1 - t^{k_i})$, dove $f(t) \in \mathbf{Z}[t]$.*

Dimostrazione. Si procede per induzione su s, il numero dei generatori di A sopra A_0. Partiamo dal caso $s = 0$; ciò significa che $A_n = 0$ per ogni $n > 0$, sicché $A = A_0$ e M è un A_0-modulo finitamente generato, e pertanto $M_n = 0$ per ogni n abbastanza grande. Dunque in questo caso $P(M, t)$ risulta un polinomio.

Supponiamo ora $s > 0$ e il teorema vero per $s - 1$. La moltiplicazione per x_s è un omomorfismo di A-moduli di M_n in M_{n+k_s}, dunque fornisce una successione esatta, diciamo

$$(1) \qquad 0 \to K_n \to M_n \xrightarrow{x_s} M_{n+k_s} \to L_{n+k_s} \to 0.$$

Poniamo $K = \bigoplus_n K_n$, $L = \bigoplus_n L_n$; essi sono entrambi A-moduli finitamente generati (poiché K è un sottomodulo e L un modulo quoziente di M), e sono annullati entrambi da x_s, sicché risultano $A_0[x_1, \ldots, x_{s-1}]$-moduli. Applicando λ alla (1) si ha, in virtú di (2.11)

$$\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0;$$

moltiplicando per t^{n+k_s} e sommando rispetto a n, si ottiene

$$(2) \qquad (1 - t^{k_s})P(M, t) = P(L, t) - t^{k_s}P(K, t) + g(t)$$

dove $g(t)$ è un polinomio. Applicando l'ipotesi induttiva, si ottiene il teorema. ∎

Denotiamo con $d(M)$ l'ordine del polo di $P(M, t)$ in $t = 1$. Esso fornisce una misura della "grandezza" di M (relativa a λ). In particolare resta definito $d(A)$. Il caso in cui tutti i gradi k_i sono uguali a 1 è particolarmente semplice:

Corollario 11.2. *Se ciascun $k_i = 1$, allora per ogni n abbastanza grande, $\lambda(M_n)$ risulta un polinomio in n (a coefficienti razionali) di grado* $d - 1$.*

Dimostrazione. In virtú di (11.1) si ha $\lambda(M_n) =$ coefficiente di t^n in $f(t) \quad (1-t)^{-s}$. Eliminando potenze di $(1-t)$ si può supporre che $s = d$ e $f(1) \neq 0$. Sia $f(t) = \sum_{k=0}^{N} a_k t^k$; poiché

$$(1-t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k$$

si ha

$$\lambda(M_n) = \sum_{k=0}^{N} a_k \binom{d+n-k-1}{d-1} \quad \text{per ogni } n \geq N,$$

e la somma al secondo membro è un polinomio in n con termine di grado massimo $(\sum a_k) n^{d-1}/(d-1)! \neq 0$. ■

Osservazioni. 1) Affinché un polinomio $f(x)$ sia tale che $f(n)$ risulti un intero per ogni intero n, non è necessario che f abbia coefficienti interi: per es., $\frac{1}{2}x(x+1)$.

2) Il polinomio di cui in (11.2) è chiamato di solito la *funzione* (o il polinomio) *di Hilbert* di M (rispetto a λ).

Ritornando ora alla successione (1), sostituiamo x_s con un qualsiasi elemento $x \in A_k$ che non sia un divisore dello zero in M (ossia, $xm = 0$ con $m \in M \Rightarrow m = 0$). Allora $K = 0$ e l'equazione (2) mostra che

$$d(L) = d(M) - 1.$$

Dunque abbiamo provato la

Proposizione 11.3. *Se $x \in A_k$ non è un divisore dello zero in M, allora $d(M/xM) = d(M) - 1$.* ■

Utilizzeremo (11.1) nel caso in cui A_0 è un anello *artiniano* (in particolare, un campo) e $\lambda(M)$ è la *lunghezza* $l(M)$ di un A_0-modulo finitamente generato M. In virtú di (6.9), $l(M)$ è additiva.

* Adottiamo qui la convenzione che il grado del polinomio nullo è -1, e inoltre che il coefficiente binomiale $\binom{n}{-1} = 0$ per $n > 0$, e $= 1$ per $n = -1$.

Esempio. Sia $A = A_0[x_1, \ldots, x_s]$, dove A_0 è un anello artiniano e le x_i sono indeterminate indipendenti. Allora A_n è un A_0-modulo libero generato dai monomi $x_1^{m_1} \ldots x_s^{m_s}$ dove $\sum m_i = n$; essi sono in totale $\binom{s+n-1}{s-1}$, dunque $P(A, t) = l(A_0)(1-t)^{-s}$.

Consideriamo ora le funzioni di Hilbert ottenute da un anello locale passando agli anelli graduati associati come si è visto nel Capitolo 10.

Proposizione 11.4. *Sia A un anello locale noetheriano,* $\mathfrak{m}$ *il suo ideale massimale,* $\mathfrak{q}$ *un ideale* $\mathfrak{m}$*-primario, M un A-modulo finitamente generato, (M_n) una* $\mathfrak{q}$*-filtrazione stabile di M. Allora:*

i) *M/M_n è di lunghezza finita, per ogni $n \geqslant 0$;*

ii) *per ogni n abbastanza grande, tale lunghezza è un polinomio $g(n)$ di grado $\leqslant s$ in n, dove s è il minimo numero di generatori di* $\mathfrak{q}$;

iii) *il grado e il coefficiente direttore di $g(n)$ dipendono soltanto da M e da* $\mathfrak{q}$, *e non dalla filtrazione scelta.*

Dimostrazione. i) Sia $G(A) = \bigoplus_n \mathfrak{q}^n/\mathfrak{q}^{n+1}$, $G(M) = \bigoplus_n M_n/M_{n+1}$. $G_0(A) = A/\mathfrak{q}$ è un anello locale artiniano, diciamo in virtú di (8.5); $G(A)$ è noetheriano e $G(M)$ è un $G(A)$-modulo graduato finitamente generato (10.22). Ciascun $G_n(M) = M_n/M_{n+1}$ è un A-modulo noetheriano annullato da $\mathfrak{q}$, dunque un $A/\mathfrak{q}$-modulo noetheriano, e quindi di lunghezza finita (poiché $A/\mathfrak{q}$ è artiniano). Pertanto M/M_n è di lunghezza finita, e

$$(1) \qquad l_n = l(M/M_n) = \sum_{r=1}^{n} l(M_{r-1}/M_r).$$

ii) Se $x_1, \ldots, x_s$ generano $\mathfrak{q}$, le immagini $\bar{x}_i$ degli x_i in $\mathfrak{q}/\mathfrak{q}^2$ generano $G(A)$ come $A/\mathfrak{q}$-algebra, e ciascun $\bar{x}_i$ ha grado 1. Dunque, in virtú di (11.2) si ha $l(M_n/M_{n+1}) = f(n)$, diciamo, dove $f(n)$ è un polinomio in n di grado $\leqslant s-1$ per ogni n abbastanza grande. Poiché dalla (1) si ha $l_{n+1} - l_n = f(n)$, ne segue che l_n è un polinomio $g(n)$ di grado $\leqslant s$, per ogni n abbastanza grande.

iii) Sia $(\tilde{M}_n)$ un'altra $\mathfrak{q}$-filtrazione stabile di M, e poniamo $\tilde{g}(n) = l(M/\tilde{M}_n)$. In virtú di (10.6) le due filtrazioni hanno differenze limitate, ossia, esiste un intero n_0 tale che $M_{n+n_0} \subseteq \tilde{M}_n$, $\tilde{M}_{n+n_0} \subseteq M_n$ per ogni $n \geqslant 0$; di conseguenza si ha $g(n+n_0) \geqslant \tilde{g}(n)$, $\tilde{g}(n+n_0) \geqslant g(n)$. Poiché g e $\tilde{g}$ sono polinomi per ogni n abbastanza grande, si ha $\lim_{n\to\infty} g(n)/\tilde{g}(n) = 1$, e pertanto $g, \tilde{g}$ hanno lo stesso grado e lo stesso coefficiente direttore. ∎

Il polinomio $g(n)$ corrispondente alla filtrazione $(\mathfrak{q}^n M)$ si denota con $\chi_{\mathfrak{q}}^M(n)$:

$$\chi_{\mathfrak{q}}^M(n) = l(M/\mathfrak{q}^n M) \qquad \text{(per ogni } n \text{ abbastanza grande).}$$

Se $M = A$, il polinomio $\chi_{\mathfrak{q}}^A(n)$ si indica semplicemente con $\chi_{\mathfrak{q}}(n)$ e prende il nome di *polinomio caratteristico* dell'ideale $\mathfrak{m}$-primario $\mathfrak{q}$. In tal caso dalla (11.4) si ha:

Corollario 11.5. *Per ogni n abbastanza grande, la lunghezza $l(A/\mathfrak{q}^n)$ è un polinomio $\chi_{\mathfrak{q}}(n)$ di grado $\leqslant s$, dove s è il minimo numero di generatori di $\mathfrak{q}$.* ∎

I polinomi $\chi_{\mathfrak{q}}(n)$ relativi a ideali $\mathfrak{m}$-primari distinti hanno tutti il medesimo grado, come mostra la seguente:

Proposizione 11.6. *Se A, $\mathfrak{m}$, $\mathfrak{q}$ sono come sopra, si ha:*

$$\deg \chi_{\mathfrak{q}}(n) = \deg \chi_{\mathfrak{m}}(n).$$

Dimostrazione. Si ha, in virtú di (7.16), $\mathfrak{m} \supseteq \mathfrak{q} \supseteq \mathfrak{m}^r$ per qualche r, da cui $\mathfrak{m}^n \supseteq \mathfrak{q}^n \supseteq \mathfrak{m}^{rn}$ e pertanto

$$\chi_{\mathfrak{m}}(n) \leqslant \chi_{\mathfrak{q}}(n) \leqslant \chi_{\mathfrak{m}}(rn) \quad \text{per ogni } n \text{ abbastanza grande.}$$

Facciamo tendere poi n all' ∞, tenendo presente che gli χ sono polinomi in n. ∎

Il grado comune dei polinomi $\chi_{\mathfrak{q}}(n)$ verrà denotato con $d(A)$: alla luce di (11.2), ciò significa che poniamo $d(A) = d(G_{\mathfrak{m}}(A))$, dove $d(G_{\mathfrak{m}}(A))$ è l'intero definito in precedenza come l'ordine del polo in $t = 1$ della serie di Poincaré di $G_{\mathfrak{m}}(A)$.

Teoria della dimensione degli anelli locali noetheriani

Sia A un anello locale noetheriano, $\mathfrak{m}$ il suo ideale massimale.

Poniamo $\delta(A) =$ minimo numero di generatori di un ideale $\mathfrak{m}$-primario di A. Ci proponiamo di dimostrare che $\delta(A) = d(A) = \dim A$. Otterremo ciò provando che $\delta(A) \geqslant d(A) \geqslant \dim A \geqslant \delta(A)$. I risultati (11.5) e (11.6) insieme, forniscono la prima relazione in tale catena:

Proposizione 11.7. $\delta(A) \geqslant d(A)$. ∎

Passiamo poi a dimostrare un risultato analogo a (11.3) per anelli locali. Si noti che la dimostrazione che daremo utilizza la versione, in forma forte, del lemma di Artin-Rees (non soltanto la parte topologica).

Proposizione 11.8. *Siano A, $\mathfrak{m}$, $\mathfrak{q}$ come sopra. Sia M un A-modulo finitamente generato, $x \in A$ un elemento non divisore dello zero in M e $M' = M/xM$. Allora*

$$\deg \chi_{\mathfrak{q}}^{M'} \leqslant \deg \chi_{\mathfrak{q}}^{M} - 1.$$

Dimostrazione. Poniamo $N = xM$; allora $N \cong M$ come A-modulo, in virtú dell'ipotesi fatta su x. Poniamo $N_n = N \cap \mathfrak{q}^n M$. Allora si ottengono successioni esatte

$$0 \to N/N_n \to M/\mathfrak{q}^n M \to M'/\mathfrak{q}^n M' \to 0.$$

Dunque, se $g(n) = l(N/N_n)$, si ha

$$g(n) - \chi_{\mathfrak{q}}^{M}(n) + \chi_{\mathfrak{q}}^{M'}(n) = 0$$

per ogni n abbastanza grande. Ora, in virtú del lemma di Artin-Rees (10.9), (N_n) è una $\mathfrak{q}$-filtrazione stabile di N. Poiché $N \cong M$, (11.4) iii) implica allora che $g(n)$ e $\chi_{\mathfrak{q}}^{M}(n)$ hanno il medesimo termine di grado massimo, donde la tesi. ■

Corollario 11.9. *Se A è un anello locale noetheriano, x un elemento non divisore dello zero in A, allora $d(A/(x)) \leqslant d(A) - 1$.*

Dimostrazione. Basta porre $M = A$ in (11.8). ■

Siamo ora in grado di dimostrare il risultato cruciale:

Proposizione 11.10. $d(A) \geqslant \dim A$.

Dimostrazione. Si procede per induzione su $d = d(A)$. Se $d = 0$, allora $l(A/\mathfrak{m}^n)$ è costante per ogni n abbastanza grande, sicché $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ per qualche n, da cui $\mathfrak{m}^n = 0$ in virtú del lemma di Nakayama (2.6). Dunque A è un anello artiniano e $\dim A = 0$.

Supponiamo $d > 0$ e sia $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \quad \subset \mathfrak{p}_r$ una catena arbitraria di ideali primi di A. Sia $x \in \mathfrak{p}_1$, $x \notin \mathfrak{p}_0$; poniamo $A' = A/\mathfrak{p}_0$, e sia x' l'immagine di x in A'. Allora $x' \neq 0$, e A' è un dominio di integrità, dunque in virtú di (11.9) si ha

$$d(A'/(x')) \leqslant d(A') - 1.$$

Inoltre, se $\mathfrak{m}'$ è l'ideale massimale di A', $A'/\mathfrak{m}'^n$ è un'immagine omomorfa di $A/\mathfrak{m}^n$, sicché $l(A/\mathfrak{m}^n) \geqslant l(A'/\mathfrak{m}'^n)$ e pertanto $d(A) \geqslant d(A')$. Di conseguenza

$$d(A'/(x')) \leqslant d(A) - 1 = d - 1.$$

Dunque, in virtú dell'ipotesi induttiva, la lunghezza di una qualsiasi catena di ideali primi in $A'/(x')$ è $\leqslant d - 1$. Ma le immagini di $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ in $A'/(x')$ formano una catena di lunghezza $r - 1$, sicché $r - 1 \leqslant d - 1$ e di conseguenza $r \leqslant d$. Dunque $\dim A \leqslant d$. ∎

Corollario 11.11. *Se A è un anello locale noetheriano,* $\dim A$ *è finita.* ∎

Se A è un anello qualsiasi, e $\mathfrak{p}$ è un ideale primo di A, allora si definisce *altezza* di $\mathfrak{p}$, e si denota con $\operatorname{ht} \mathfrak{p}$, l'estremo superiore delle lunghezze delle catene di ideali primi $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \quad \subset \mathfrak{p}_r = \mathfrak{p}$ che terminano in $\mathfrak{p}$: stante (3.13), $\operatorname{ht} \mathfrak{p} = \dim A_{\mathfrak{p}}$. Dunque, da (11.11) segue:

Corollario 11.12. *In un anello noetheriano ogni ideale primo ha altezza finita, e pertanto l'insieme degli ideali primi in un anello noetheriano soddisfa la condizione della catena discendente.* ∎

Osservazione. Similmente si definisce la *profondità* di $\mathfrak{p}$, che si denota con depth $\mathfrak{p}$, considerando le catene ascendenti di ideali primi che partono da $\mathfrak{p}$: chiaramente depth $\mathfrak{p} = \dim A/\mathfrak{p}$. Tuttavia la profondità di un ideale primo, perfino in un anello noetheriano, può essere infinita (a meno che l'anello non sia locale). Cfr. l'Esercizio 4.

Proposizione 11.13. *Sia A un anello locale noetheriano di dimensione d. Allora esiste un ideale $\mathfrak{m}$-primario in A generato da d elementi x_1, x_d, e pertanto* $\dim A \geqslant \delta(A)$.

Dimostrazione. Costruiamo gli elementi $x_1, \ldots, x_d$ induttivamente, in modo tale che ogni ideale primo contenente $(x_1, \ldots, x_i)$ abbia altezza $\geqslant i$, per ogni i. Supponiamo $i > 0$ e $x_1, \ldots, x_{i-1}$ già costruiti. Siano $\mathfrak{p}_j$ $(1 \leqslant j \leqslant s)$ i primi minimali (se ne esistono) dell'ideale $(x_1, \ldots, x_{i-1})$ che hanno altezza *esattamente* $i - 1$. Poiché $i - 1 < d = \dim A = \operatorname{ht} \mathfrak{m}$, si ha $\mathfrak{m} \neq \mathfrak{p}_j$ $(1 \leqslant j \leqslant s)$, sicché $\mathfrak{m} \neq \bigcup_{j=1}^{s} \mathfrak{p}_j$, in virtú di (1.11). Scegliamo un elemento $x_i \in \mathfrak{m}$, con $x_i \notin \bigcup \mathfrak{p}_j$, e sia $\mathfrak{q}$ un arbitrario ideale primo contenente $(x_1, \ldots, x_i)$. Allora $\mathfrak{q}$ contiene qualche ideale primo minimale $\mathfrak{p}$ di $(x_1, \ldots, x_{i-1})$. Se $\mathfrak{p} = \mathfrak{p}_j$ per qualche j, si ha $x_i \in \mathfrak{q}$, $x_i \notin \mathfrak{p}$, sicché $\mathfrak{q} \supset \mathfrak{p}$ e pertanto ht $\mathfrak{q} \geqslant i$; se $\mathfrak{p} \neq \mathfrak{p}_j$ $(1 \leqslant j \leqslant s)$, allora ht $\mathfrak{p} \geqslant i$, dunque ht $\mathfrak{q} \geqslant i$. Pertanto ogni ideale primo contenente $(x_1, \ldots, x_i)$ ha altezza $\geqslant i$.

Consideriamo allora l'ideale $(x_1, \ldots, x_d)$. Se $\mathfrak{p}$ è un primo minimale di tale ideale, $\mathfrak{p}$ ha altezza $\geqslant d$, sicché $\mathfrak{p} = \mathfrak{m}$ (infatti $\mathfrak{p} \subset \mathfrak{m} \Rightarrow$ $\Rightarrow \text{ht}\,\mathfrak{p} < \text{ht}\,\mathfrak{m} = d$). Dunque l'ideale $(x_1, \ldots, x_d)$ è $\mathfrak{m}$-primario. ∎

Teorema 11.14. (Teorema della dimensione). *Per un arbitrario anello locale noetheriano A i seguenti tre interi sono uguali tra loro:*

i) *la massima lunghezza delle catene di ideali primi in A;*

ii) *il grado del polinomio caratteristico $\chi_{\mathfrak{m}}(n) = l(A/\mathfrak{m}^n)$;*

iii) *il minimo numero di generatori di un ideale $\mathfrak{m}$-primario di A.*

Dimostrazione. Utilizzare (11.7), (11.10), (11.13). ∎

Esempio. Sia A l'anello di polinomi $k[x_1, \ldots, x_n]$ localizzato nell'ideale massimale $(x_1, \ldots, x_n)$ e sia $\mathfrak{m}$ il suo ideale massimale. Allora $G_{\mathfrak{m}}(A)$ è un anello di polinomi in n indeterminate e quindi la sua serie di Poincaré è $(1-t)^{-n}$. Da ciò, utilizzando l'equivalenza di (i) e (ii) in (11.14), si deduce che $\dim A = n$.

Corollario 11.15. $\dim A \leqslant \dim_k (\mathfrak{m}/\mathfrak{m}^2)$.

Dimostrazione. Se gli elementi $x_i \in \mathfrak{m}$ $(1 \leqslant i \leqslant s)$ sono tali che le loro immagini in $\mathfrak{m}/\mathfrak{m}^2$ formano una base di tale spazio vettoriale, allora gli x_i generano $\mathfrak{m}$ in virtú di (2.8); dunque $\dim_k (\mathfrak{m}/\mathfrak{m}^2) =$ $= s \geqslant \dim A$, stante (11.13). ∎

Corollario 11.16. *Sia A un anello noetheriano, e siano $x_1, \ldots,$ $x_r \in A$. Allora ogni ideale primo minimale $\mathfrak{p}$ appartenente a $(x_1, \ldots, x_r)$ ha altezza $\leqslant r$.*

Dimostrazione. In $A_{\mathfrak{p}}$ l'ideale $(x_1, \ldots, x_r)$ diventa $\mathfrak{p}^e$-primario, dunque $r \geqslant \dim A_{\mathfrak{p}} = \text{ht}\,\mathfrak{p}$. ∎

Corollario 11.17. (Teorema dell'ideale principale di Krull). *Sia A un anello noetheriano e sia x un elemento di A non divisore dello zero né invertibile. Allora ogni ideale primo minimale $\mathfrak{p}$ di (x) ha altezza* 1.

Dimostrazione. In virtú di (11.16), ht $\mathfrak{p} \leqslant 1$. Se ht $\mathfrak{p} = 0$, allora $\mathfrak{p}$ è un ideale primo appartenente a 0, sicché ogni elemento di $\mathfrak{p}$ è un divisore dello zero, stante (4.7): ciò è una contraddizione, giacché $x \in \mathfrak{p}$. ■

Corollario 11.18. *Sia A un anello locale noetheriano, x un elemento di $\mathfrak{m}$ non divisore dello zero. Allora* $\dim A/(x) = \dim A - 1$.

Dimostrazione. Poniamo $d = \dim A/(x)$. In virtú di (11.9) e (11.14) si ha $d \leqslant \dim A - 1$. D'altra parte, siano x_i $(1 \leqslant i \leqslant d)$ elementi di $\mathfrak{m}$ le cui immagini in $A/(x)$ generano un ideale $\mathfrak{m}/(x)$-primario. Allora l'ideale $(x, x_1, \ldots, x_d)$ di A è $\mathfrak{m}$-primario, dunque $d + 1 \geqslant \dim A$. ■

Corollario 11.19. *Sia $\hat{A}$ il completamento $\mathfrak{m}$-adico di A. Allora* $\dim A = \dim \hat{A}$.

Dimostrazione. Si ha, in virtú di (10.15), $A/\mathfrak{m}^n \cong \hat{A}/\hat{\mathfrak{m}}^n$, da cui $\chi_{\mathfrak{m}}(n) = \chi_{\hat{\mathfrak{m}}}(n)$. ■

Se $x_1, \ldots, x_d$ generano un ideale $\mathfrak{m}$-primario, e $d = \dim A$, si dice che $x_1, \ldots, x_d$ costituiscono un *sistema di parametri*. Essi possiedono una certa proprietà di indipendenza descritta nella proposizione seguente.

Proposizione 11.20. *Siano $x_1, \ldots, x_d$ un sistema di parametri per A e sia $\mathfrak{q} = (x_1, \ldots, x_d)$ l'ideale $\mathfrak{m}$-primario da essi generato. Sia $f(t_1, \ldots, t_d)$ un polinomio omogeneo di grado s a coefficienti in A, e supponiamo che*

$$f(x_1, \ldots, x_d) \in \mathfrak{q}^{s+1}.$$

Allora tutti i coefficienti di f appartengono a $\mathfrak{m}$.

Dimostrazione. Consideriamo l'epimorfismo di anelli graduati

$$\alpha\colon (A/\mathfrak{q})[t_1, \ldots, t_d] \to G_{\mathfrak{q}}(A)$$

dato da $t_i \mapsto \bar{x}_i$, dove le t_i sono indeterminate e $\bar{x}_i$ è x_i mod $\mathfrak{q}$. L'ipotesi su f implica che $\bar{f}(t_1, \ldots, t_d)$ (la riduzione di f mod $\mathfrak{q}$) appartiene al nucleo di α. Supponiamo per assurdo che qualche coefficiente di f sia invertibile, allora $\bar{f}$ non è un divisore dello zero (cfr. Capitolo 1, Esercizio 3). Ebbene si ha

$$\begin{aligned} d(G_{\mathfrak{q}}(A)) &\leqslant d((A/\mathfrak{q})[t_1, \ldots, t_d]/(\bar{f})) \quad \text{poiché } \bar{f} \in \operatorname{Ker}(\alpha) \\ &= d((A/\mathfrak{q})[t_1, \ldots, t_d]) - 1 \quad \text{stante (11.3)} \\ &= d - 1 \quad \text{in virtú dell'esempio che segue (11.3).} \end{aligned}$$

Ma $d(G_q(A)) = d$, in virtú del teorema fondamentale (11.14). Ciò fornisce la contraddizione richiesta. ■

La proposizione precedente assume una forma semplice se A contiene un campo k che risulta isomorfo nell'applicazione quoziente al campo residuo $A/\mathfrak{m}$:

Corollario 11.21. *Se $k \subset A$ è un campo che risulta isomorfo nell'applicazione quoziente ad $A/\mathfrak{m}$, e se $x_1, \ldots, x_d$ è un sistema di parametri, allora gli elementi $x_1, \ldots, x_d$ sono algebricamente indipendenti sopra k.*

Dimostrazione. Supponiamo che $f(x_1, \ldots, x_d) = 0$, dove f è un polinomio a coefficienti in k. Se $f \not\equiv 0$, si può scrivere $f = f_s +$ termini di grado piú alto, dove f_s è omogeneo di grado s e $f_s \not\equiv 0$. Applicando (11.20) a f_s, si deduce che f_s ha tutti i suoi coefficienti in $\mathfrak{m}$. Poiché f_s ha i coefficienti in k, ciò implica che $f_s \equiv 0$, ossia una contraddizione. Dunque $x_1, \ldots, x_d$ sono algebricamente indipendenti su k. ■

Anelli locali regolari

In geometria algebrica vi è una distinzione importante tra punti *singolari* e *non singolari* (cfr. Esercizio 1). Gli anelli locali dei punti non singolari hanno come loro generalizzazione (al caso non geometrico) i cosiddetti anelli locali *regolari*: si tratta degli anelli che soddisfano una qualsiasi delle condizioni (equivalenti) i)-iii) del teorema seguente.

Teorema 11.22. *Sia A un anello locale noetheriano di dimensione d, $\mathfrak{m}$ il suo ideale massimale, $k = A/\mathfrak{m}$. Allora le seguenti condizioni sono equivalenti:*

i) $G_\mathfrak{m}(A) \cong k[t_1, \ldots, t_d]$ *dove le t_i sono indeterminate indipendenti*;
ii) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = d$;
iii) $\mathfrak{m}$ *può essere generato da d elementi.*

Dimostrazione. i) $\Rightarrow$ ii) è chiaro. ii) $\Rightarrow$ iii) in virtú di (2.8): cfr. la dimostrazione di (11.15). iii) $\Rightarrow$ i): sia $\mathfrak{m} = (x_1, \ldots, x_d)$, allora, stante (11.20), l'applicazione $\alpha: k[x_1, \ldots, x_d] \to G_\mathfrak{m}(A)$ è un isomorfismo di anelli graduati. ■

Un anello locale regolare è necessariamente un *dominio di integrità*; ciò è una conseguenza del risultato piú generale:

Lemma 11.23. *Sia A un anello, $\mathfrak{a}$ un ideale di A tale che $\bigcap_n \mathfrak{a}^n = 0$. Supponiamo che $G_\mathfrak{a}(A)$ sia un dominio di integrità. Allora A è un dominio di integrità.*

Dimostrazione. Siano x, y elementi non nulli di A. Allora poiché $\bigcap \mathfrak{a}^n = 0$, esistono degli interi $r, s \geqslant 0$ tali che $x \in \mathfrak{a}^r, x \notin \mathfrak{a}^{r+1}$, $y \in \mathfrak{a}^s, y \notin \mathfrak{a}^{s+1}$. Denotiamo con $\bar{x}, \bar{y}$, rispettivamente, le immagini di x, y in $G_r(A)$, $G_s(A)$. Allora $\bar{x} \neq 0, \bar{y} \neq 0$, sicché $\bar{x}\,\bar{y} = \overline{xy} \neq 0$, da cui $xy \neq 0$. ∎

Ne segue, stante (9.2), che gli anelli locali regolari di dimensione 1 sono precisamente gli anelli di valutazione discreta.

Si può dimostrare inoltre che se A è un anello locale e $G_\mathfrak{m}(A)$ è un dominio di integrità integralmente chiuso, allora A è integralmente chiuso. Dunque un anello locale regolare è integralmente chiuso; tuttavia esistono domini locali integralmente chiusi di dimensione > 1 che non sono regolari.

Proposizione 11.24. *Sia A un anello locale noetheriano. Allora A è regolare se e soltanto se $\hat{A}$ è regolare.*

Dimostrazione. In virtú di (10.16), (10.26) e (11.19) si ha che $\hat{A}$ è un anello locale noetheriano della stessa dimensione di A e con ideale massimale $\hat{\mathfrak{m}}$. Ora, utilizzando (10.22) che asserisce che $G_\mathfrak{m}(A) \cong$ $\cong G_{\hat{\mathfrak{m}}}(\hat{A})$, si ottiene il risultato. ∎

Osservazioni. 1) Da quanto detto sopra segue che anche $\hat{A}$ è un dominio di integrità. Geometricamente, ciò significa che (localmente)

"non singolarità" $\Rightarrow$ "irriducibilità analitica"

ossia che, in un punto non singolare, vi è un unico "ramo" analitico.

2) Se A contiene un campo k che risulta isomorfo nell'applicazione quoziente ad $A/\mathfrak{m}$ (caso geometrico), allora (11.22) implica che $\hat{A}$ è un anello di serie di potenze formali su k in d indeterminate. Dunque i completamenti degli anelli locali di punti non singolari su una varietà d-dimensionale sopra k sono tutti isomorfi.

Esempio. Sia $A = k[x_1, \ldots, x_n]$ (essendo k un campo arbitrario, e le x_i indeterminate indipendenti); sia $\mathfrak{m} = (x_1, \ldots, x_n)$. Allora $A_\mathfrak{m}$ (l'anello locale dello spazio affine k^n nell'origine) è un anello locale regolare: infatti $G_\mathfrak{m}(A)$ è un anello di polinomi in n variabili.

Dimensione trascendente

Concludiamo questa breve trattazione della teoria della dimensione mostrando come la dimensione degli anelli locali si raccorda con la dimensione di una varietà definita classicamente mediante il campo delle funzioni.

Supponiamo per semplicità che k sia algebricamente chiuso e sia V una varietà affine irriducibile sopra k. Dunque l'anello delle coordinate $A(V)$ è della forma

$$A(V) = k[x_1, \ldots, x_n]/\mathfrak{p}$$

dove $\mathfrak{p}$ è un ideale primo. Il campo delle frazioni del dominio di integrità $A(V)$ è chiamato il campo delle funzioni razionali su V e si denota con $k(V)$. Esso è un'estensione finitamente generata di k e quindi ha un grado di trascendenza finito su k — il numero massimo di elementi algebricamente indipendenti. Tale numero è per definizione la *dimensione* di V. Ricordiamo ora che, in virtú del teorema degli zeri di Hilbert, i punti di V corrispondono biunivocamente agli ideali massimali di $A(V)$. Se P è un punto con ideale massimale $\mathfrak{m}$, chiameremo *dimensione locale* di V in P l'intero $\dim A(V)_{\mathfrak{m}}$. Ci proponiamo di provare il

Teorema 11.25. *Per una qualsiasi varietà irriducibile V sopra k, la dimensione locale di V in un punto arbitrario è uguale a* $\dim V$.

Osservazione. Già sappiamo, in virtú di (11.21), che $\dim V \geqslant \dim A_{\mathfrak{m}}$ per ogni $\mathfrak{m}$. Il problema è di dimostrare la disuguaglianza opposta, e a tale scopo il lemma fondamentale è:

Lemma 11.26. *Siano $B \subseteq A$ domini di integrità con B integralmente chiuso e A intero su B. Sia $\mathfrak{m}$ un ideale massimale di A, e poniamo $\mathfrak{n} = \mathfrak{m} \cap B$. Allora $\mathfrak{n}$ è massimale e* $\dim A_{\mathfrak{m}} = \dim B_{\mathfrak{n}}$.

Dimostrazione. La tesi segue facilmente dai risultati del Capitolo 5. Innanzitutto $\mathfrak{n}$ è massimale, stante (5.8). Inoltre, se

$$\mathfrak{m} \supset \mathfrak{q}_1 \supset \mathfrak{q}_2 \supset \quad \supset \mathfrak{q}_d \tag{1}$$

è una catena strettamente decrescente di ideali primi in A, la sua intersezione con B risulta, in virtú di (5.9), una catena strettamente decrescente di ideali primi

$$\mathfrak{n} \supset \mathfrak{p}_1 \supset \mathfrak{p}_2 \supset \quad \supset \mathfrak{p}_d. \tag{2}$$

Ciò prova che $\dim B_n \geqslant \dim A_m$. Viceversa, data la catena (2), è possibile, in virtú di (5.16), sollevare questa in una catena (1) (necessariamente strettamente decrescente): dunque $\dim A_m \geqslant \dim B_n$. ■

Passiamo ora alla:

Dimostrazione di (11.25). In virtú del Lemma di normalizzazione (Capitolo 5, Esercizio 16), è possibile trovare un anello di polinomi $B = k[x_1, \ldots, x_d]$ contenuto in $A(V)$ tale che $d = \dim V$ e $A(V)$ è intero su B. Poiché B è integralmente chiuso (cfr. l'osservazione che segue (5.12)) si può applicare (11.26), sicché basta provare (11.25) per l'anello B, ossia per lo spazio affine. Ma ogni punto dello spazio affine può essere assunto come origine delle coordinate e, come si è già visto, $k[x_1, \ldots, x_d]$ localizzato nell'ideale massimale $(x_1, \ldots, x_d)$ è un anello locale di dimensione d. ■

Corollario 11.27. *Per ogni ideale massimale* $\mathfrak{m}$ *di* $A(V)$ *si ha*:

$$\dim A(V) = \dim A(V)_\mathfrak{m}.$$

Dimostrazione. Per definizione si ha $\dim A(V) = \sup_\mathfrak{m} \dim A(V)_\mathfrak{m}$. Ma in virtú di (11.25) tutti gli anelli $A(V)_\mathfrak{m}$ hanno la medesima dimensione. ■

Esercizi

1. Sia $f \in k[x_1, \ldots, x_n]$ un polinomio irriducibile sopra un campo k algebricamente chiuso. Un punto P sulla varietà $f(x) = 0$ è *non singolare* $\Leftrightarrow$ non tutte le derivate parziali $\partial f/\partial x_i$ si annullano in P. Sia $A = k[x_1, \ldots, x_n]/(f)$, e sia $\mathfrak{m}$ l'ideale massimale di A corrispondente al punto P. Provare che P è non singolare $\Leftrightarrow A_\mathfrak{m}$ è un anello locale regolare.
[In virtú di (11.18) si ha $\dim A_\mathfrak{m} = n - 1$. Ora
$$\mathfrak{m}/\mathfrak{m}^2 \cong (x_1, \ldots, x_n)/(x_1, \ldots, x_n)^2 + (f)$$
e ha dimensione $n - 1$ se e soltanto se $f \notin (x_1, \ldots, x_n)^2$.]

2. In (11.21) supponiamo che A sia completo. Dimostrare che l'omomorfismo $k[[t_1, \ldots, t_d]] \to A$ dato da $t_i \mapsto x_i$ $(1 \leqslant i \leqslant d)$ è iniettivo e che A è un modulo finitamente generato sopra $k[[t_1, t_d]]$. [Utilizzare (10.24).]

3. Estendere (11.25) ad un campo non algebricamente chiuso. [Se $\bar{k}$ è la chiusura algebrica di k, allora $\bar{k}[x_1, \ldots, x_n]$ è intero su $k[x_1, \ldots, x_n]$.]

4. Un esempio di dominio noetheriano di dimensione infinita (Nagata). Sia k un campo e sia $A = k[x_1, x_2, \ldots, x_n, \ldots]$ un anello di polinomi su k in una infinità numerabile di indeterminate. Sia $m_1, m_2, \ldots$ una successione crescente di interi positivi tale che $m_{i+1} - m_i > m_i - m_{i-1}$ per ogni $i > 1$. Poniamo $\mathfrak{p}_i = (x_{m_i+1}, \ldots, x_{m_{i+1}})$ e sia S il complementare in A dell'unione degli ideali $\mathfrak{p}_i$.
   Ogni $\mathfrak{p}_i$ è un ideale primo e pertanto S è una parte moltiplicativa. L'anello $S^{-1}A$ è noetheriano (cfr. Capitolo 7, Esercizio 9). Ogni ideale $S^{-1}\mathfrak{p}_i$ ha altezza uguale a $m_{i+1} - m_i$, dunque $\dim S^{-1}A = \infty$.

5. Riformulare (11.1) mediante il gruppo di Grothendieck $K(A_0)$ (Capitolo 7, Esercizio 25).

6. Sia A un anello (non necessariamente noetheriano). Provare che

$$1 + \dim A \leqslant \dim A[x] \leqslant 1 + 2 \dim A.$$

   [Sia $f: A \to A[x]$ l'immersione canonica e consideriamo la fibra di $f^*: \mathrm{Spec}\,(A[x]) \to \mathrm{Spec}\,(A)$ sopra un ideale primo $\mathfrak{p}$ di A. Tale fibra può essere identificata con lo spettro di $k \otimes_A A[x] \cong k[x]$, dove k è il campo residuo in $\mathfrak{p}$ (Capitolo 3, Esercizio 21), e $\dim k[x] = 1$. Ora utilizzare l'Esercizio 7 del Capitolo 2.]

7. Sia A un anello noetheriano. Allora

$$\dim A[x] = 1 + \dim A,$$

   e quindi, per induzione su n,

$$\dim A[x_1, \ldots, x_n] = n + \dim A.$$

   [Sia $\mathfrak{p}$ un ideale primo di altezza m in A. Allora esistono elementi $a_1, \ldots, a_m \in \mathfrak{p}$ tali che $\mathfrak{p}$ è un ideale primo minimale appartenente all'ideale $\mathfrak{a} = (a_1, \ldots, a_m)$. In virtù dell'Esercizio 7 del Capitolo 4, $\mathfrak{p}[x]$ è un ideale primo minimale di $\mathfrak{a}[x]$ e pertanto $\mathrm{ht}\,\mathfrak{p}[x] \leqslant m$. D'altra parte, una catena di ideali primi $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_m = \mathfrak{p}$ dà origine ad una catena $\mathfrak{p}_0[x] \subset \ldots \subset \mathfrak{p}_m[x] = \mathfrak{p}[x]$, sicché $\mathrm{ht}\,\mathfrak{p}[x] \geqslant m$. Dunque $\mathrm{ht}\,\mathfrak{p}[x] = \mathrm{ht}\,\mathfrak{p}$. Ora utilizzare l'argomentazione dell'Esercizio 6.]

Appendice all'edizione italiana

DI PAOLO MAROSCIA

Premessa

Lo scopo principale dell'Appendice è quello di aiutare il lettore della versione italiana del testo di Atiyah e Macdonald, da un lato, ad inquadrare (anche storicamente) alcuni metodi e risultati fondamentali nello studio degli anelli commutativi (e dei moduli definiti su di essi), e dall'altro, ad avere una visione d'insieme, sia pure sintetica e necessariamente parziale, della situazione attuale dell'Algebra commutativa: problemi aperti, indirizzi di ricerca, nuove tendenze, rapporti con altre discipline...

L'Appendice è divisa in cinque sezioni. La prima ha carattere introduttivo e contiene, tra l'altro, una breve discussione sui rapporti tra l'Algebra commutativa e le due discipline per tradizione piú strettamente legate ad essa: la Teoria algebrica dei numeri e la Geometria algebrica. Nella sezione 2 viene tratteggiato rapidamente lo sviluppo dell'Algebra commutativa, dai primi lavori di Hilbert fino agli inizi degli anni '50, ossia prima dell'avvento dell'Algebra omologica. La sezione 3 è dedicata interamente all'esposizione di nozioni e risultati fondamentali di algebra omologica riguardanti lo studio degli anelli commutativi; occorre sottolineare che tale esposizione, se da un lato rende piú agevole ed efficace la presentazione degli argomenti, non segue, in realtà, lo sviluppo storico delle idee: infatti, storicamente, il punto di partenza è stato proprio lo studio degli anelli locali regolari, i quali si trovano qui trattati alla fine! Nella sezione 4 vi è un'ampia introduzione allo studio delle "risoluzioni libere finite", nonché una breve discussione di taluni problemi di carattere omologico, di grande attualità e interesse, relativi ai moduli definiti su anelli noetheriani. Infine la sezione 5 (che può riguardarsi, almeno in parte, come una sezione di applicazioni) è dedicata all'esame di alcune questioni relative alle varietà intersezioni complete e alla fattorialità.

Oltre ai numerosi riferimenti sparsi nel testo, l'Appendice contiene alla fine un'ampia bibliografia che, speriamo, riuscirà utile al lettore, il quale voglia orientarsi nella vastissima letteratura esistente. Tale bibliografia naturalmente non ha alcuna pretesa di completezza, soprattutto per quanto riguarda gli "articoli vari": anzi, ci scusiamo fin d'ora per le inevitabili omissioni.

Occorre aggiungere inoltre che la necessità di contenere il lavoro entro limiti ragionevoli, ci ha costretto a fare delle scelte precise sugli argomenti da trattare. Così purtroppo, non siamo riusciti a includere nell'Appendice alcuni argomenti pur di notevole importanza, quali, ad esempio, la teoria dei campi, la teoria degli invarianti, la K-teoria algebrica e la teoria dei gruppi di Brauer: per tali argomenti, ci siamo limitati a fornire qua e là alcune brevi indicazioni.

Per concludere, desidero ringraziare i professori D. Buchsbaum e A. Seidenberg per le cordiali e stimolanti discussioni avute con loro durante la preparazione del lavoro. Ringrazio in modo particolare il professor P. Salmon, che mi ha incoraggiato nella stesura della versione finale del lavoro, dandomi altresí numerosi consigli e preziosi suggerimenti.

Paolo Maroscia

Waltham, Massachusetts
dicembre 1979

1.

Brevi considerazioni generali

Alcune "novità"

Si può dire oggi, completando un'affermazione contenuta all'inizio di [1], che l'Algebra commutativa è essenzialmente lo studio degli anelli commutativi, con particolare riguardo ai moduli definiti su di essi.[1]

L'importanza sempre piú grande assegnata, negli ultimi trenta anni, ai moduli anziché agli ideali, è senza dubbio uno degli aspetti "nuovi" piú rilevanti dell'algebra commutativa. Si tratta di una tendenza la quale prosegue, a sua volta, la tendenza alla "linearizzazione" che caratterizza i lavori di E. Noether e di W. Krull (senza voler risalire a Hilbert e a Macaulay) e che si è rafforzata notevolmente con la nascita e il successivo sviluppo della cosiddetta Algebra omologica, a partire dagli inizi degli anni '50.

Il primo testo organico su tale argomento, che ha dato anche il nome alla nuova disciplina, è l'*Homological Algebra* di H. Cartan e S. Eilenberg. In esso vengono esposte per la prima volta, inquadrate in una teoria piú generale, e precisamente nel contesto dei funtori[2] additivi e dei loro funtori "derivati", varie teorie particolari: la coomologia dei gruppi, la coomologia delle algebre associative, la coomologia delle algebre di Lie, la teoria delle sizigie di Hilbert, ecc...; in particolare, vengono introdotti i funtori $\mathrm{Tor}_n(M, N)$ e $\mathrm{Ext}^n(M, N)$.

[1] Per quanto riguarda specificamente la teoria dei campi, oltre ai testi citati in bibliografia ([5], [9], [10], [14], [15], [79],...), si veda: E. Artin, *Galois Theory*, Notre Dame Math. Lect. *2*, 2ª ed., Univ. of Notre Dame Press, Indiana 1966 e M. Nagata, *Field Theory*, Dekker, New York 1977.

[2] Le nozioni di categoria e di funtore erano state introdotte pochi anni prima da S. Eilenberg e S. Mac Lane ("Trans. Amer. Math. Soc.", *58*, 1945, pp. 231-294), con riferimento al problema dell'assiomatizzazione della teoria dei gruppi di omologia e coomologia degli spazi topologici (cfr., ad es., [58]).

Inoltre, tale testo ha funzionato da catalizzatore, sia in campo algebrico che in campo geometrico. In particolare, A. Grothendieck, attraverso l'introduzione e lo studio sistematico delle "categorie abeliane" [177], ha potuto far rientrare nell'Algebra omologica la teoria della coomologia di uno spazio a coefficienti in un fascio di gruppi abeliani e, in pari tempo, J. P. Serre si è servito in modo sistematico dell'Algebra omologica in Geometria algebrica [233] e in Geometria analitica [232], oltre che in Algebra commutativa ([52], [234], [235]).

Altri aspetti "nuovi" che hanno arricchito notevolmente l'Algebra commutativa sono legati all'introduzione della nozione di *fascio* (in particolare, di fascio coerente) effettuata sistematicamente da H. Cartan intorno al 1950 [3] e della nozione generale di *spazio anellato*,[4] dovuta essenzialmente a Cartan e a Serre, intorno al 1953, e piú tardi largamente generalizzata da H. Grauert e da Grothendieck, ricorrendo ad una categoria piú ampia di spazi anellati con fibre eventualmente non ridotte, cioè contenenti elementi nilpotenti.[5]

Come conseguenza di tutto ciò, sono emersi, tra l'altro, punti di vista e criteri orientativi del tutto nuovi:

a) un risultato è "valido", soprattutto perché è funtoriale;

b) una proprietà è "interessante", specialmente se ha carattere locale[6];

c) la ricerca di enunciati sempre piú generali, senza restrizioni di comodo;

d) lo studio di legami piú stretti e profondi con altri rami della matematica.[7]

Rapporti con altre discipline

Come si è visto in precedenza, alcuni cambiamenti notevoli in Algebra commutativa sono avvenuti grazie all'influenza dell'Al-

[3] Tale nozione era stata già introdotta in topologia, da J. Leray, nel 1945.

[4] Essa rispondeva all'esigenza di generalizzare la nozione di varietà analitica complessa, allo scopo di poter considerare anche delle singolarità, come in geometria algebrica.

[5] La presenza di elementi nilpotenti, insieme alla considerazione di punti non "chiusi", avrebbe costituito piú tardi uno degli aspetti "rivoluzionari" della geometria algebrica, fondata sulla nozione di *schema* [101].

[6] Quale, ad es., la proiettività, la piattezza, la nozione di anello di Cohen-Macaulay, di anello di Gorenstein, di dominio integralmente chiuso, ecc...

[7] Cfr. J. Dieudonné, *Panorama des mathématiques pures*, Gauthier-Villars, Paris 1977. Segnaliamo inoltre un breve articolo di M. F. Atiyah, alquanto stimolante: *The unity of mathematics*, "Bull. London Math. Soc.", *10*, 1978, pp. 69-76.

gebra omologica, della Geometria algebrica e della Geometria analitica.[8]

Passiamo ora a sviluppare ulteriori considerazioni, in relazione ad altre discipline, partendo dai rapporti tra l'Algebra commutativa e la Teoria algebrica dei numeri. Riguardo a ciò, forse si può affermare che, mentre fino ai primi decenni del secolo, tali rapporti erano stati *diretti* ed *espliciti* (basti pensare, per es., alla nozione di elemento intero su un anello, ai moduli sugli anelli principali, agli anelli e moduli noetheriani, agli anelli di Dedekind, agli anelli di frazioni, alle estensioni di campi, ecc...), oggi essi appaiono invece, per cosí dire, *mediati*[9] in primo luogo, attraverso la geometria algebrica o l'algebra omologica (non commutativa).

Un esempio illuminante è fornito dalla sistemazione data da Grothendieck alla Geometria algebrica negli Elementi [100], in cui viene inglobata molta parte della Teoria algebrica dei numeri (realizzando, tra l'altro, un antico sogno di Kronecker [193]). Piú in particolare, possiamo citare in proposito:

a) la risoluzione, ad opera di P. Deligne, delle celebri Congetture di Weil, relative al numero delle soluzioni di equazioni polinomiali sopra un campo finito (cfr. [93, vol. I], [103] e, per un'ampia introduzione all'argomento: A. D. Thomas, *Zeta functions: an introduction to algebraic geometry*, Pitman, London 1977);

b) l'enorme sviluppo dello studio di problemi diofantéi in geometria algebrica, sulla scia dei primi risultati ottenuti tra il 1920 e il 1930 da L. J. Mordell, A. Weil e C. L. Siegel (cfr. S. Lang, *Diophantine Geometry*, Interscience, New York 1962)[10];

c) la riscoperta avvenuta verso la metà degli anni '50, ad opera di K. Iwasawa e H. W. Leopoldt, della teoria dei campi ciclotomici[11],

[8] Conviene sottolineare inoltre che esistono numerose e notevoli applicazioni dell'Algebra commutativa alla Geometria analitica, in particolare alla Geometria analitica locale, ossia allo studio locale degli insiemi analitici (o insiemi degli zeri di funzioni analitiche). Si veda in proposito: S. S. ABHYANKAR, *Local analytic geometry*, Academic Press, New York/London 1964 e H. GRAUERT-R. REMMERT, *Analytische Stellenalgebren*, Springer, Berlin 1971.

[9] Segnaliamo in proposito la soluzione ottenuta, con l'uso di metodi analitici, da H. M. STARK ("Michigan Math. J.", *14*, 1967, pp. 1-27) del classico problema di determinare completamente le estensioni quadratiche immaginarie del campo razionale che hanno *numero di classe* 1 [1, Cap. 9].

[10] Per avere un'idea generale di come concetti e metodi di geometria algebrica possano essere utilizzati in problemi di teoria dei numeri, cfr. H. P. F. SWINNERTON-DYER, *Applications of Algebraic Geometry to Number Theory*, in *1969 Number Theory Institute*, in "Amer. Math. Soc. Proc. Symp. Pure Math.", *20*, 1971, pp. 1-52.

[11] Che risale essenzialmente a E. KUMMER, verso la metà del secolo scorso.

e i legami di tale teoria, e dei suoi successivi sviluppi, con lo studio degli anelli degli endomorfismi delle varietà abeliane (cfr., ad es., G. Shimura, *Automorphic functions and number theory*, Lect. Notes Math., *54*, Springer, Berlin 1968);

d) l'utilizzazione sistematica in teoria dei numeri, oltre che in algebra commutativa e in geometria algebrica, di metodi e risultati di coomologia dei gruppi: si veda ad es. [71] e, per un'ampia e dettagliata trattazione (orientata verso la *Teoria del corpo di classe*): E. Weiss, *Cohomology of groups*, Academic Press, New York and London 1969; segnaliamo infine una ricca esposizione di carattere storico di S. Mac Lane: *Origins of the cohomology of groups*, in "Enseignement Math.", *24*, 1978, pp. 1-29.

Per finire, si può aggiungere che la stessa *Teoria del corpo di classe* può essere considerata, almeno in parte, come un capitolo di "algebra astratta", soprattutto per il suo carattere unificante nella Teoria algebrica dei numeri.[12]

Anche per quanto riguarda l'influenza della Geometria algebrica sull'Algebra commutativa, c'è stata, in un certo senso, un'evoluzione. Precisamente, superata l'epoca "classica", diciamo tra il 1920 e il 1930 (in cui, in breve, problemi di geometria algebrica venivano tradotti in problemi relativi agli ideali in anelli di polinomi, e viceversa), tale influenza è diventata forse meno *diretta* (soprattutto a causa dei metodi e delle tecniche nuove che hanno via via arricchito la Geometria algebrica) ma pur sempre riconoscibile, a volte addirittura "trasparente".

Uno degli esempi forse più significativi a riguardo è fornito dallo studio delle proprietà algebriche delle varietà di Grassmann.[13] Precisamente, si è dimostrato che ogni varietà siffatta è proiettivamente normale (Igusa, 1953 [192]), è proiettivamente fattoriale (Andreotti e Salmon, 1957 [131], e più tardi Samuel, 1964 [51]), è proiettivamente di Cohen-Macaulay (Hochster, 1972 [189]) e infine è proiettivamente

[12] Per un'introduzione alla teoria del corpo di classe dei campi di numeri algebrici, si veda: G. J. Janusz, *Algebraic number fields*, Academic Press, New York 1973. Per un'esposizione sistematica, cfr. [71], [83] e soprattutto: E. Artin, J. Tate, *Class field theory*, Benjamin, New York 1968.

[13] Tale studio ha seguito di pari passo lo sviluppo e l'approfondimento delle proprietà geometriche di siffatte varietà (cfr. [220]). Per la definizione e le proprietà fondamentali delle varietà di Grassmann, si veda: W. V. D. Hodge, D. Pedoe, *Methods of algebraic geometry*, vol. II, Cambridge Univ. Press, 1952 o anche S. Kleiman, D. Laksov, *Schubert calculus*, in "Amer. Math. Monthly", *79*, 1972, pp. 1061-1082.

di Gorenstein (in virtú di un risultato generale di Murthy [206]). Un altro esempio è dato dai problemi "classici" tuttora aperti, relativi alle curve, e piú in generale, alle varietà algebriche intersezioni complete, e la cui formulazione in termini algebrici è addirittura elementare, come si vedrà piú avanti nella sezione 5. E poi ancora, gli stessi "teoremi di struttura" ottenuti recentemente da Buchsbaum e Eisenbud (cfr. la successiva sez. 4) possono essere collegati, in un certo senso, con un problema estremamente attuale in geometria algebrica: lo studio delle sottovarietà di codimensione > 1 di una varietà algebrica.

I problemi sopra accennati sono tipici problemi riguardanti i fondamenti della geometria algebrica classica che si traducono in termini di teoria degli ideali. L'impostazione piú astratta e generale di tali fondamenti, data da Serre e da Grothendieck, ha portato alla formulazione di nuovi problemi di algebra commutativa, alcuni dei quali di grande respiro, tra cui in primo luogo la "Congettura di Serre" che ha svolto altresí un ruolo trainante nello sviluppo di altre teorie, quali l'Algebra omologica e la K-Teoria algebrica.[14] Adesso si assiste in geometria algebrica ad un "ritorno al concreto"[15] o meglio, riprendendo un'espressione estremamente efficace di O. Zariski (*Collected Papers*, vol. I, The MIT Press, 1972, p. XIII): "... There are signs at the present moment of the pendulum swinging back from 'schemes', 'motives',[16] and so on toward concrete but difficult unsolved questions concerning the old pedestrian concept of a projective variety (and even of algebraic surfaces)." In particolare, è difficile prevedere se ciò porterà a sviluppi dell'algebra commutativa simili ai precedenti: al momento attuale, forse si può dire soltanto che è l'algebra omologica, piú che la geometria algebrica, a "trascinare" l'algebra commutativa.

Infine occorre segnalare che ulteriori originali contributi sono stati apportati all'Algebra commutativa dalla K-Teoria algebrica (cfr. [226]). Si tratta di una "nuova" disciplina, la quale, secondo un'opi-

[14] Tale congettura, che si trova enunciata in [233], afferma che "ogni modulo proiettivo di tipo finito sull'anello dei polinomi $k[x_1, \ldots, x_n]$ in n indeterminate a coefficienti in un campo k arbitrario, è libero, $\forall n > 1$"; essa è stata dimostrata nel 1976 da D. QUILLEN [221] e indipendentemente da A. A. SUSLIN [238].

[15] Segnaliamo in proposito che recentemente (cfr. Sém. Bourbaki, novembre 1979) W. FULTON e P. DELIGNE hanno dimostrato una classica "Congettura di Zariski", secondo cui "se C è una curva nel piano proiettivo complesso P^2 dotata al piú di soli punti doppi ordinari, allora il gruppo fondamentale $\pi_1(P^2 - C)$ è abeliano".

[16] Si veda, ad es., M. DEMAZURE, *Motifs des variétés algébriques*, Lect. Notes Math. *180*, Springer, Berlin 1971, pp. 19-38.

nione comune dei matematici, ha avuto inizio, al pari della K-Teoria topologica (M. F. Atiyah-F. Hirzebruch, *Vector bundles and homogeneous spaces*, in "Amer. Math. Soc. Proc. Symp. Pure Math.", *3*, 1961, pp. 7-38), con la dimostrazione data da Grothendieck del Teorema di Riemann-Roch (cfr. [143]). In tale occasione egli introdusse il funtore K, ora chiamato K_0: si veda in proposito [1, Cap. 7, Esercizio 26]. Da allora, la K-Teoria algebrica ha avuto degli sviluppi notevolissimi, legati in parte ai tentativi di risoluzione della Congettura di Serre sui moduli proiettivi.[17]

Conclusioni

Come già abbiamo detto nella premessa introduttiva, numerosi sono i problemi e i risultati che non siamo neppure riusciti a sfiorare nelle pagine che seguono. Tuttavia, anche per ragioni di completezza, non possiamo fare a meno di accennare brevemente ad alcuni tra i piú importanti di essi (altri ancora saranno citati nel testo, piú avanti):

a) Problemi relativi ai gruppi algebrici lineari e alla teoria degli invarianti: cfr. [22], [29], [89], [105], [110], [220]. Si veda inoltre: C. Procesi, *Algebre cicliche e problema di Lüroth*, XI Congresso UMI, Palermo 1979, in "Boll. UMI" (in corso di stampa), nonché J. E. Humphreys, *Hilbert's fourteenth problem*, in "Amer. Math. Monthly" *85*, 1978, pp. 341-353.

b) Studio di alcune classi notevoli di anelli (non noetheriani), con particolare riguardo agli anelli di Krull ([3], [23]), gli anelli di valutazione ([21], [48]) e, collegati ad essi, gli anelli di Bézout[18] e di Prüfer ([6], [26], [36]), gli anelli henseliani (cfr. [47] e S. Greco, *Anelli henseliani*, in *Categories and Commutative Algebra*, Cremonese, Roma 1974) e gli anelli coerenti (cfr. [3], [56] e J. P. Soublin, *Anneaux et modules cohérents*, in "J. Algebra", *15*, 1970, pp. 455-472).

c) Problemi di "cancellazione": per un'esposizione generale, si veda [164]; ci limitiamo qui ad enunciare un risultato ottenuto recentemente da Miyanishi e Fujita, secondo cui "se A è un anello commutativo, finitamente generato su un campo perfetto[19] k, tale che $A[X]\cong$

[17] Si veda: R. G. Swan, *Algebraic K-Theory*, in "Proc. Internat. Congress Math." (Nice 1970), vol. I, Gauthier-Villars, Paris 1971, pp. 191-199 e H. Bass (a cura di), *Algebraic K-Theory*, I, II, III, Lect. Notes Math., *341*, *342*, *343*, Springer, Berlin 1973.

[18] Ricordiamo (cfr. [6]) che l'anello di tutti gli interi algebrici e l'anello delle funzioni trascendenti intere sono entrambi anelli di Bézout.

[19] Per la definizione di campo perfetto, si veda, ad es., [15, vol. I].

$\cong k[U, V, W]$, essendo X, U, V, W indeterminate, allora risulta: $A \cong k[S, T]$, con S e T indeterminate".[20]

d) Questioni riguardanti la "piattezza normale": si tratta di un argomento, il cui studio, iniziato col celebre lavoro di Hironaka [186], è stato poi sviluppato da vari autori; per un'esposizione generale, contenente anche la discussione di taluni tra i principali problemi aperti in tale ambito, si veda: L. Robbiano-G. Valla, *Teoria della piattezza normale: alcuni aspetti e problemi*, in "Sem. Ist. Mat. Univ. Genova", *8*, 1978.

e) Questioni di natura topologica legate allo spettro primo di un anello: il risultato fondamentale ottenuto in proposito è un teorema di caratterizzazione degli *spazi spettrali* (ossia spazi topologici omeomorfi allo spettro primo di un anello commutativo, dotato della topologia di Zariski) dimostrato da M. Hochster in [187]; si veda inoltre [29] e R. Wiegand, *Prime ideal structure in Noetherian rings*, in [40].[21]

f) Applicazioni di metodi omologici in algebra commutativa alle Teorie combinatorie: si tratta di un indirizzo recente e alquanto promettente, nel quale sono stati ottenuti finora numerosi risultati, ad opera soprattutto di R. Stanley, G. Reisner e M. Hochster (si veda: M. Hochster, *Cohen-Macaulay rings, combinatorics, and simplicial complexes*, in [40]).

[20] Tale risultato mi è stato segnalato da D. Mumford.

[21] Per analoghi problemi relativi allo spettro primo considerato come insieme parzialmente ordinato, si veda: M. Fontana, *Sopra alcuni problemi relativi agli insiemi spettrali*, in "Rend. Sem. Fac. Sc. Univ. Cagliari", *49*, 1979, pp. 445-467.

2.

Cenni sulla situazione dell'algebra commutativa agli inizi degli anni '50

Introduzione

La scelta di tale periodo come punto di riferimento per abbozzare un quadro d'insieme dell'algebra commutativa è giustificata, a nostro parere, da varie considerazioni:

a) Innanzitutto, proprio in quel periodo, si assiste alla nascita dell'*algebra omologica*, che tanta influenza avrebbe dovuto avere non soltanto sull'Algebra commutativa, ma anche in Geometria algebrica e in Geometria analitica: in particolare, tra il 1950 e il 1953 viene preparato il trattato fondamentale di Cartan e Eilenberg [59], che verrà pubblicato piú tardi, nel 1956.

b) Nel 1953 appare l'*Ideal Theory* di Northcott, contenente un'esposizione succinta ed elegante dei risultati fondamentali relativi agli ideali negli anelli noetheriani, nonché due capitoli dedicati rispettivamente agli anelli locali regolari e ai completamenti. Si tratta tuttavia di un libro scritto in un'ottica "classica", anche se non del tutto privo di collegamenti con le tematiche piú geometriche dell'algebra commutativa[1]: tra l'altro, vengono omessi alcuni argomenti di rilievo, quali ad es. la teoria delle valutazioni, i teoremi di Cohen-Seidenberg, le funzioni di Hilbert, e manca addirittura la nozione di modulo. Si può dire brevemente che l'*Ideal Theory* chiude l'era pre-omologica dell'Algebra commutativa.

c) Qualche anno prima, nel 1946, era apparso il celebre trattato di Weil [126], in cui, tra l'altro, veniva introdotta per la prima volta la

[1] Per es., vengono introdotti gli elementi "analiticamente indipendenti" utilizzati da Zariski nella caratterizzazione geometrica degli anelli locali regolari. In ogni caso, occorrerà attendere la fine degli anni '50 per disporre di un trattato di algebra commutativa chiaramente orientato verso la geometria algebrica [15], grazie soprattutto all'influenza e all'opera di Zariski.

nozione di varietà algebrica "astratta" (ottenuta incollando pezzi affini) e veniva costruita la geometria algebrica sopra un campo arbitrario[2]: in particolare, veniva sviluppata la teoria dei divisori e una teoria generale delle intersezioni (fino ad allora una tale teoria era stata costruita, limitatamente al caso di una varietà proiettiva non singolare, da van der Waerden). Siamo così, in geometria algebrica, all'inizio di una svolta "storica": per le tappe successive, cfr. [233], [100], [87].

d) Nel 1951 viene pubblicato il volume di Chevalley [91], il quale contiene una trattazione sistematica della teoria dei campi di funzioni algebriche di una variabile sopra un campo base arbitrario, in modo puramente algebrico: per es., manca del tutto la nozione e perfino il termine di "curva algebrica". Esso occupa un posto a sé nello sviluppo storico dell'algebra e della geometria algebrica, anche per le difficoltà di estendere i metodi e le tecniche usate da Chevalley alle varietà algebriche di dimensione > 1.

Ora, allo scopo di inquadrare meglio storicamente sia il contenuto di [1], sia le considerazioni sviluppate nelle sezioni successive, accenneremo rapidamente ai principali risultati noti all'epoca,[3] passando in rassegna alcuni lavori fondamentali (si veda in proposito una esposizione di carattere storico di I. Kaplansky [19, pp. 153-166], a cui ci siamo in parte ispirati).

L'opera di David Hilbert

Ci limiteremo qui ad accennare a due celebri memorie [184] e [185], pubblicate rispettivamente nel 1890 e nel 1893.[4]

[2] Occorre aggiungere che, negli anni intorno al 1930, van der Waerden aveva fatto numerosi progressi in una tale costruzione. Inoltre tutto ciò sarebbe stato inglobato e largamente generalizzato, a partire dalla fine degli anni '50, negli Elementi di GROTHENDIECK [100], in cui viene operata una rifondazione completa ed estremamente generale dell'intera Geometria algebrica (cfr. per una prima esposizione di carattere generale: A. GROTHENDIECK, *The cohomology theory of abstract algebraic varieties*, in "Proc. Internat. Congr. Math.", Edinburgh 1958).

[3] Segnaliamo che il trattato di KRULL [8] contiene, oltre a note storiche, un'esposizione dei risultati ottenuti, nell'ambito della teoria degli ideali, fino al 1935.

[4] Non si può fare a meno di citare altresì due memorie fondamentali, una di KRONECKER [193] e l'altra di DEDEKIND e WEBER [160], apparse entrambe nel 1882. La prima si proponeva di rifondare e di unificare, per mezzo di nozioni e metodi algebrici, sia la Teoria dei numeri che la Geometria algebrica, mentre la seconda si proponeva di dimostrare in modo puramente algebrico, a partire da un'estensione finita del campo delle funzioni razionali $C(X)$, i principali risultati ottenuti da Riemann per le curve (in particolare, si ritrova il Teorema di Riemann-Roch, insieme a numerosi altri risultati fondamentali).

Nella prima si trovano numerosi risultati; in particolare:

i) si dimostra che "ogni ideale dell'anello dei polinomi $\mathbf{C}[X_1, \ldots, X_n]$ è finitamente generato",[5] risultato che sarà successivamente generalizzato sotto la forma del cosiddetto "teorema della base di Hilbert". Conviene sottolineare che Hilbert era condotto a tali ricerche dal problema di dimostrare che gli anelli degli invarianti dei gruppi di matrici sono finitamente generati[6] (ciò che piú tardi avrebbe fatto parte del XIV problema di Hilbert [42]);

ii) vengono studiati i moduli di sizigie, ottenuti a partire dalle relazioni o *sizigie* esistenti tra i generatori, diciamo $f_1, \ldots, f_h$ di un ideale dell'anello di polinomi $A = \mathbf{C}[X_1, \ldots, X_n]$, della forma: $a_1 f_1 + \ldots + a_h f_h = 0$, con $a_1, \ldots, a_h \in A$. Ebbene, Hilbert provò che tali moduli (costituiti dalle h-uple $(a_1, \ldots, a_h)$) sono ancora finitamente generati, sicché è possibile considerare le *seconde* sizigie e cosí via (giacché anche i successivi moduli di sizigie sono finitamente generati) e per di piú che, dopo n passi, si ottiene il modulo nullo.

iii) viene introdotto essenzialmente il *polinomio caratteristico* [1, Coroll. 11.2], considerando una varietà proiettiva V di $\mathbf{P}^n_{\mathbf{C}}$, definita da un certo ideale omogeneo $\mathfrak{a}$ di $S = \mathbf{C}[X_0, \ldots, X_n]$ e il numero delle ipersuperfici linearmente indipendenti di un dato ordine m in $\mathbf{P}^n$, per $m \gg 1$, che contengono la varietà in questione. Precisamente, Hilbert prova che la dimensione dello spazio vettoriale complesso $\bar{S}_m = S_m/(S_m \cap \mathfrak{a})$, dove S_m denota lo spazio vettoriale dei polinomi omogenei di grado m di S, è un intero, il quale, *per m abbastanza grande*, può essere rappresentato con un polinomio in m:

$$\lambda(\bar{S}_m) = a_0\binom{m}{r} + a_1\binom{m}{r-1} + \quad + a_r,$$

dove $a_1, \ldots, a_r$ sono interi e r è la dimensione di V.

La seconda memoria contiene il celebre *Nullstellensatz* [1, Coroll. 7.10], il quale stabilisce una corrispondenza biunivoca tra gli ideali massimali dell'anello $K[X_1, \ldots, X_n]$, essendo K un campo algebricamente chiuso arbitrario, e i punti dello spazio affine $\mathbf{A}^n_K$; da ciò segue, inoltre, una corrispondenza biunivoca tra gli ideali radicali

[5] Tra l'altro, ciò risolveva completamente un problema posto da Cayley e Kronecker relativo all'espressione di una curva algebrica sghemba irriducibile (di uno spazio a tre dimensioni) come intersezione di un numero finito di superfici algebriche.

[6] Per alcuni notevoli sviluppi ottenuti recentemente in proposito, cfr. [29], [191] e un lavoro di G. Kempf ("Michigan Math. J.", *26*, 1979, pp. 19-32).

(risp. primi) dell'anello $K[X_1, \ldots, X_n]$ e le varietà algebriche (risp. le varietà algebriche irriducibili) di $\mathbf{A}^n_K$.

Conviene sottolineare che esiste anche una versione "omogenea" del Nullstellensatz per le varietà algebriche proiettive[7] (cfr. ad es. [94] oppure [103]), nonché una versione "analitica", per un ideale proprio dell'anello dei germi di funzioni numeriche, analitiche nell'origine di $\mathbf{C}^n$, $O_n = \mathbf{C}\{x_1, \ldots, x_n\}$.[8]

Gli sviluppi successivi fino a Emmy Noether

Partendo dal Teorema degli zeri di Hilbert, il quale può anche enunciarsi dicendo che "se f è un polinomio dell'anello $\mathbf{C}[X_1, \ldots, X_n]$ che si annulla in tutti i punti di $\mathbf{C}^n$ in cui si annullano i polinomi di un ideale $\mathfrak{a}$ di $\mathbf{C}[X_1, \ldots, X_n]$, allora una potenza di f appartiene ad $\mathfrak{a}$", Lasker fu condotto nel 1905 (cfr. [199]) a definire la nozione di ideale primario in un anello di polinomi e a dimostrare, tra l'altro, che "ogni ideale nell'anello $\mathbf{C}[X_1, \ldots, X_n]$ può esprimersi come un'intersezione finita di ideali primari".

Un posto a sé, storicamente molto importante, occupa il classico trattato di Macaulay [37], il quale racchiude i risultati di numerose ricerche dell'autore, tra i quali ci limitiamo qui a ricordare:

i) il celebre *Teorema della purezza*, secondo cui "*se $\mathfrak{a}$ è un ideale dell'anello* $\mathbf{C}[X_1, \ldots, X_n]$ *di altezza h e generato da h elementi, allora $\mathfrak{a}$ risulta un ideale puro*[9]";

ii) la non esistenza di un estremo superiore per il numero dei generatori richiesti per gli ideali primi dell'anello $\mathbf{C}[X, Y, Z]$ e della sua localizzazione $\mathbf{C}[X, Y, Z]_{(X, Y, Z)}$.[10]

[7] Una nuova e semplice dimostrazione di tale risultato, da cui si deduce in particolare il teorema principale della Teoria dell'eliminazione, è stata data recentemente da P. Cartier e J. Tate ("Enseignement Math.", *24*, 1978, pp. 311-317).

[8] In proposito, si veda ad es.: J. C. Tougeron, *Idéaux de fonctions différentiables*, Springer, Berlin 1972, in cui, tra l'altro, vengono usati con profitto metodi e risultati di algebra locale e di algebra omologica per lo studio dell'anello dei germi di funzioni numeriche, derivabili indefinitamente nell'origine di $\mathbf{R}^n$.

[9] Un ideale $\mathfrak{a}$ di un anello noetheriano A arbitrario si dice *puro*, se tutti gli ideali primi associati ad $\mathfrak{a}$ [1, Cap. 4] hanno la medesima altezza ($=$ ht $\mathfrak{a}$).

[10] Piú precisamente, Macaulay costruí degli esempi i quali mostravano che, per ogni intero n fissato ($n > 0$), esiste un ideale primo $\mathfrak{p}$ di altezza 2 in $\mathbf{C}[X, Y, Z]$ tale che $\mathfrak{p}$, e perfino $\mathfrak{p}\mathbf{C}[X, Y, Z]_{(X, Y, Z)}$, non può essere generato da n elementi. Per un'esposizione moderna e dettagliata di tali esempi, cfr. [19, pp. 1-16] oppure [174]. Segnaliamo infine che analoghi esempi di ideali primi nell'anello $k[[x, y, z]]$, essendo k un campo di caratteristica zero arbitrario, sono stati ottenuti recentemente da T. T. Moh ("J. Math. Soc. Japan" *26*, 1974, pp. 722-734).

Ma il primo grande contributo allo sviluppo dell'algebra commutativa è dovuto senz'altro a Emmy Noether, di cui ci limitiamo qui a citare brevemente tre lavori: [213], [214], [215].

Nel primo vengono studiati gli anelli in cui ogni ideale è finitamente generato, ossia, in modo equivalente, gli anelli che soddisfano alla condizione della catena ascendente per gli ideali,[11] i quali saranno chiamati appunto anelli noetheriani; in tal modo, veniva assunto come assioma proprio la tesi del Teorema della base di Hilbert.[12] In particolare, per ogni ideale di un anello siffatto viene dimostrata l'esistenza di una decomposizione primaria, nonché l'unicità delle componenti primarie isolate.[13]

Il secondo lavoro contiene il classico Lemma di normalizzazione, relativo ad una k-algebra integra finitamente generata su un campo *infinito* k (per ulteriori estensioni di tale risultato, cfr. [12]).

Nel terzo lavoro si trova una trattazione assiomatica degli anelli di Dedekind, sviluppata a partire dagli anelli di interi algebrici, nonché la nozione generale di elemento intero su un anello (estesa poi da Krull a quella di elemento intero su un ideale).

C'è da aggiungere inoltre che E. Noether fu la prima ad osservare che le rappresentazioni di un gruppo finito G in un campo k corrispondono ai moduli sull'algebra-gruppo $k[G]$, che è un anello artiniano. Tale legame ha determinato successivamente nuove direzioni di ricerca nella teoria degli anelli artiniani e, al tempo stesso, ha fornito un nuovo e interessante punto di vista nella teoria delle rappresentazioni dei gruppi.

Infine, occorre menzionare il famoso trattato di van der Waerden

[11] Gli anelli soddisfacenti alla condizione della catena discendente per gli ideali furono introdotti alcuni anni dopo da E. ARTIN in [132]; la ben nota caratterizzazione ([1, Th. 8.5]) è dovuta ad AKIZUKI (1935).

[12] Molti anni piú tardi, un fatto analogo sarebbe accaduto per il Teorema della purezza di Macaulay, cosí da pervenire ai cosiddetti anelli di MACAULAY [6] o di COHEN-MACAULAY [11].

[13] Si noti che in [1] il Teor. 7.13 viene ottenuto ripetendo la dimostrazione originaria di E. Noether, che poggia sulla nozione di ideale irriducibile (nozione che svolge un ruolo importante, come vedremo, nello studio degli anelli di Gorenstein); invece il risultato relativo alla "parziale" unicità delle componenti è ottenuto in [1] con un'altra dimostrazione (piú generale), basata sulle proprietà degli anelli di frazioni. Forse è il caso di aggiungere a questo proposito che le prime proprietà di un anello di frazioni rispetto ad una parte moltiplicativa, priva di divisori dello zero, sono state date da H. GRELL, un allievo di E. Noether, nel 1927 e sono state poi riprese ed estese da CHEVALLEY e finalmente, in tutta generalità, da A. I. UZKOV (*On rings of quotients of commutative rings*, in "Mat. Sbornik N. S.", *13*, 1943, pp. 71-78).

[14], la cui prima edizione apparve tra il 1930 e il 1931, non soltanto per una esposizione più avanzata e talvolta una nuova elaborazione di alcuni risultati e idee di E. Noether, ma anche per i legami tra certi argomenti ivi trattati e talune questioni di geometria algebrica.

L'opera di Wolfgang Krull

Si devono a Krull molti lavori, taluni di importanza davvero fondamentale per lo sviluppo dell'Algebra commutativa (e alcuni altri forse non ancora sufficientemente esplorati). Ci limiteremo qui a citare solo alcuni di essi.

Il primo lavoro di rilievo [194] è del 1928. Esso contiene, tra l'altro, il celebre *Teorema dell'ideale principale* (*Hauptidealsatz*) [1, Cor. 11.17]. Come giustamente osserva Kaplansky in [6], quest'ultimo risultato "is probably the most important single theorem in the theory of Noetherian rings".[14] Infatti, per convincersene, basta elencare alcune delle sue più importanti conseguenze:

(A) Ogni ideale primo di un anello noetheriano ha altezza finita,[15] ossia, in modo equivalente, ogni anello noetheriano semilocale ha dimensione di Krull finita.[16]

(B) Gli ideali primi di un anello noetheriano soddisfano la d.c.c., anzi una forma più ristretta di questa, nel senso che le catene *massimali* o *saturate* di ideali primi contenute in un ideale primo assegnato hanno tutte la medesima lunghezza (ciò che non è più vero per le catene massimali di ideali primi contenenti un ideale primo assegnato): cfr. ad es. [12] e più in generale [46].

(C) Se $\mathfrak{p}_1$ e $\mathfrak{p}_2$ sono ideali primi in un anello noetheriano A tali che esiste un ideale primo $\mathfrak{p}$ con la proprietà: $\mathfrak{p}_1 \subset \mathfrak{p} \subset \mathfrak{p}_2$, allora esistono in A infiniti ideali primi siffatti.[16 bis]

[14] D'altra parte, già Northcott aveva osservato in [13] che, prima di tale teorema "a Noetherian ring had been a kind of pale shadow of a polynomial ring".

[15] Ciò che non è più vero nel caso non noetheriano, giacché esistono (cfr. [3, Capp. 5-6, p. 176]) anelli di valutazione con uno spettro dato da una catena della forma: $0 \subset \ldots \subset \mathfrak{p}_n \subset \mathfrak{p}_{n-1} \subset \ldots \subset \mathfrak{p}_1 \subset \mathfrak{m}$ (essendo $\mathfrak{m}$ l'ideale massimale): ciò mostra altresì che esistono domini non noetheriani privi di ideali primi di altezza 1.

[16] Conviene aggiungere che in realtà Krull ha dimostrato per di più che "l'altezza di un ideale primo $\mathfrak{p}$ di un anello noetheriano è il minimo intero n tale che $\mathfrak{p}$ è minimale su un ideale generato da n elementi".

[16 bis] Cfr. nota 15.

(D) Un dominio di integrità noetheriano A è fattoriale, ossia un dominio a fattorizzazione unica (brevemente, un UFD), se e soltanto se, ogni ideale primo di altezza 1 di A è principale.[17]

(E) Se A è un anello noetheriano di dimensione finita, si ha (cfr. [6] oppure [1, Cap. 11, Es. 7]):

$$\dim A[X] = \dim A + 1,$$ [18]

da cui, per induzione:

$$\dim A[X_1, \ldots, X_n] = \dim A + n.$$

(F) Sia A un dominio di integrità noetheriano e K il suo campo dei quozienti. Allora K è una A-algebra finitamente generata,[19] se e soltanto se, A ha dimensione ≤ 1 e possiede soltanto un numero finito di ideali massimali (cfr. [6, Th. 146]).

(G) Se A è un anello (noetheriano) di Cohen-Macaulay, allora tale risulta l'anello $A[X]$ (cfr. [6, Th. 151]).

[17] Ricordiamo che un dominio di integrità A si dice un UFD, se verifica le seguenti condizioni:

a) ogni elemento non invertibile di A è un prodotto finito di fattori *irriducibili* (ossia, elementi non invertibili, divisibili soltanto per se stessi e per elementi invertibili);

b) ogni elemento irriducibile di A è *primo* (ossia, genera un ideale primo). Si noti che, stante la a), la b) risulta equivalente alla b′): "la fattorizzazione, di cui in a), è unica, a meno dell'ordine dei fattori e di fattori invertibili".

Passiamo ora a dimostrare l'enunciato (D).

Se A è un UFD, certamente ogni ideale primo di altezza 1 è principale: basta considerare un ideale $\mathfrak{p}$ siffatto e decomporre un suo elemento non nullo arbitrario in fattori primi (senza sfruttare l'ipotesi di noetherianità).

Viceversa, essendo A noetheriano, la a) è chiaramente soddisfatta; d'altra parte, se q è un arbitrario elemento irriducibile, esiste certamente un ideale primo $\mathfrak{p}$ di altezza 1 contenente q (in virtú dell'Hauptidealsatz), ma $\mathfrak{p}$ è principale, per ipotesi, donde la conclusione.

[18] Per un'estensione di tale formula al caso non noetheriano, insieme ad alcuni risultati generali, cfr. [230] e [231].

[19] Tale proprietà, riferita ad un dominio di integrità arbitrario, è stata assunta in [6] come assioma di definizione di una vasta classe di domini: i cosiddetti G-domini; dunque la (F) è una caratterizzazione dei G-domini noetheriani. Tale enunciato si trova dimostrato per la prima volta in una classica Nota di Artin-Tate [133], in relazione ad un risultato di Zariski [1, Prop. 7.9], a sua volta collegato ad una nuova dimostrazione del Nullstellensatz data dallo stesso Zariski (cfr. "Bull. Amer. Math. Soc.", *53*, 1947). Per quanto riguarda il comportamento dei G-domini generali (non noetheriani) cfr. ad es. [6], nonché P. Maroscia, *Some results on G-domains*, "Boll. UMI", *17*-B, 1980, pp. 1166-1177.

Tra gli altri lavori di Krull segnaliamo, oltre al trattato [8], il lavoro [196] del 1938, dedicato agli anelli locali, non necessariamente noetheriani. In esso, tra l'altro, viene introdotta la tecnica del completamento di un anello locale e viene studiata per la prima volta la nozione di anello locale regolare, ossia di un anello locale noetheriano di dimensione n tale che il suo ideale massimale è generato esattamente da n elementi.[90] In particolare, si dimostra in tale lavoro che:

i) un anello locale regolare è un dominio integralmente chiuso;

ii) se A è un anello locale regolare e $\mathfrak{p}$ è un ideale primo arbitrario di A, si ha:

$$\dim A = \operatorname{ht}\mathfrak{p} + \dim A/\mathfrak{p}.$$

Conviene sottolineare che l'importanza e l'interesse della nozione di anello locale regolare (nonché della teoria della dipendenza integrale) in geometria algebrica, furono scoperti poco dopo da Zariski: in particolare, egli dimostrò (cfr. [248]) che l'anello locale di un punto semplice di una varietà algebrica è regolare, tale proprietà essendo altresí caratteristica, se il campo base è perfetto.

D'altra parte, Krull aveva sollevato due questioni relative agli anelli locali regolari, dette anche "congetture di Krull" (anche se non sembra che Krull le abbia mai enunciate sotto forma di congetture), le quali avrebbero svolto in seguito un ruolo notevole nello sviluppo dell'Algebra locale:

1) Ogni localizzazione $A_{\mathfrak{p}}$ di un anello locale regolare A rispetto ad un suo ideale primo $\mathfrak{p}$ arbitrario, è ancora un anello locale regolare.

2) Ogni anello locale regolare è un UFD.

Per finire, citiamo sommariamente alcuni contributi ulteriori di Krull, e precisamente:

a) la caratterizzazione di un dominio noetheriano integralmente chiuso come intersezione di anelli di valutazione discreta (cfr. [195]), punto di partenza per lo studio dei cosiddetti anelli di Krull (cfr. [3, Ch. 7] oppure [23]);

b) l'introduzione e lo studio delle valutazioni[91] aventi gruppi di valori arbitrari e degli anelli di valutazione (cfr. [195]);

[90] Tuttavia la terminologia introdotta da Krull per tale classe di anelli era leggermente diversa: l'attributo "regolare" fu introdotto piú tardi da Chevalley in [151] (sia pure in un senso un po' ristretto).

[91] O meglio, valutazioni di Krull, per distinguerle dalle valutazioni ordinarie chiamate anche "valori assoluti", poiché includonó, tra l'altro, l'usuale valore assoluto: le prime (in particolare i corrispondenti anelli di valutazione) svolgono

c) il cosiddetto "teorema dell'intersezione" [1, Teorema 10.17];

d) i teoremi del "going-up" e del "going-down", successivamente estesi da Cohen e Seidenberg in [156], al caso in cui gli anelli in questione contengono divisori dello zero[22];

e) il risultato secondo cui "la chiusura integrale di un dominio noetheriano locale di dimensione 1 è ancora un dominio noetheriano", generalizzato successivamente da Akizuki, dando origine al noto Teorema di Krull-Akizuki (cfr. [12]);

f) l'introduzione e lo studio degli anelli di Jacobson, sviluppato in [197].[23]

Alcuni risultati successivi

Passiamo ora ad accennare rapidamente all'opera di O. Zariski, nonché ad alcuni contributi di C. Chevalley, I. S. Cohen e P. Samuel (limitatamente al periodo in esame, ossia, fino agli inizi degli anni '50).

A Zariski spetta innanzitutto il merito di aver scoperto l'esistenza di legami profondi ed estremamente fecondi tra l'algebra commutativa e la geometria algebrica, e più in generale, di aver rifondato la geometria algebrica su solide basi algebriche. In particolare, numerosi e penetranti sono i contributi da lui dati, soprattutto all'Algebra locale. In breve, si può affermare che l'influenza di Zariski sullo sviluppo dell'algebra commutativa è stata senza dubbio non minore di quella di Krull o dei suoi predecessori.

Ci limitiamo qui a ricordare, tra l'altro:

a) il celebre "main theorem"[24] ("Trans. Amer. Math. Soc.", *53*, 1943, pp. 490-542), che forse può essere considerato il risultato più

/

un ruolo importante in Algebra commutativa e in Geometria algebrica; mentre le seconde intervengono soprattutto nella Teoria algebrica dei numeri (cfr. ad es. [84]).

[22] Si noti che in [156] le dimostrazioni sviluppate sono alquanto più semplici di quelle date da Krull e inoltre vengono discussi alcuni interessanti controesempi relativi all'enunciato del "going-down", i quali mostrano che nessuna delle ipotesi che ivi compaiono può essere omessa.

[23] Nello stesso anno 1951, tali anelli venivano introdotti e studiati, indipendentemente, con la denominazione di anelli di Hilbert (in quanto strettamente legati al Nullstellensatz), da O. Goldman ("Math. Z.", *54*, 1951, pp. 136-140).

[24] Cfr. anche [111]; inoltre in [47] viene riportata un'estensione di tale risultato dovuta a C. Peskine. Segnaliamo infine che un'interessante versione "non commutativa" del "main theorem" è stata data recentemente da M. Artin e W. Schelter ("Amer. J. Math.", *101*, 1979, pp. 301-330).

importante ottenuto da Zariski nello studio delle varietà normali[25]: egli era stato condotto a tale studio dal problema di dare una dimostrazione della risoluzione delle singolarità di una superficie su un campo algebricamente chiuso di caratteristica zero arbitrario, problema che egli riuscí a risolvere nel 1939 ("Annals of Math.", *40*, 1939, pp. 639-689);

b) il contributo e l'impulso notevoli dati in [248] allo studio degli anelli locali regolari (introdotti da Krull) e in particolare, la dimostrazione ivi sviluppata, limitatamente agli anelli locali regolari "geometrici" della "congettura di Krull" secondo cui "ogni localizzazione di un anello locale regolare rispetto ad un ideale primo è ancora un anello locale regolare";

c) l'uso sistematico in geometria algebrica degli anelli di valutazione e piú esattamente dei "posti" ad essi associati, effettuato per la prima volta nel lavoro: *Foundations of a general theory of birational correspondences*, in "Trans. Amer. Math. Soc.", *53*, 1943, pp. 490-542;

d) l'introduzione e lo studio di una vasta classe di anelli noetheriani in [247], i quali saranno chiamati poi "anelli di Zariski" da Samuel in [229], dove lo studio di tali anelli viene ulteriormente sviluppato e approfondito (per la definizione, si veda [1, Cap. 10, Esercizio 6]);

e) un risultato collegato a uno di Chevalley, citato piú avanti, secondo cui (cfr. [249]) "il completamento di un dominio locale geometrico integralmente chiuso è un dominio di integrità", ossia [15, vol. II] il dominio locale di partenza è *analiticamente irriducibile*;

f) il lavoro [250] in cui si dimostra, tra l'altro, che "se l'anello locale $O_{V,P}$ di un punto P di una varietà algebrica V è integralmente chiuso (ossia, V è localmente normale in P), allora il completamento di $O_{V,P}$ è ancora integralmente chiuso".

Per finire, occorre segnalare ancora il contributo dato da Zariski (cfr. [248]) alla risoluzione dell'altra "congettura di Krull", relativa alla fattorialità degli anelli locali regolari. Precisamente, egli dimostrò che l'anello locale di un punto semplice è un UFD e inoltre che, per provare la congettura in generale, basta far vedere che ogni anello locale regolare di dimensione 3 è un UFD (per ulteriori osservazioni in proposito, cfr. [15, vol. II, p. 313]).

[25] Ossia normali in ogni punto. Una notevole proprietà di tali varietà è stata dimostrata da A. SEIDENBERG ("Trans. Amer. Math. Soc.", *69*, 1950, pp. 357-386): precisamente "se V è una varietà proiettiva irriducibile normale di $\mathbf{P}_k^n$, con k campo algebricamente chiuso, allora l'intersezione di V con un iperpiano "generico" di $\mathbf{P}^n$ è ancora una varietà irriducibile e normale".

Passando ora ad accennare ai contributi di Chevalley, ricordiamo innanzitutto lo studio approfondito degli anelli (noetheriani) locali e semilocali effettuato in [151].[26] In particolare, Chevalley si rese conto che la nozione di anello semilocale è una buona generalizzazione della nozione di anello locale: per es. un'estensione (intera e) finita di un anello semilocale è ancora semilocale (mentre un'estensione finita di un anello locale non è locale, in generale), inoltre il completamento di un anello semilocale è non soltanto semilocale e della stessa dimensione, ma è addirittura una somma diretta di anelli locali[27] e infine, per un anello semilocale, è possibile costruire una buona teoria della dimensione (cfr. ad es. [20]).

In un'altra fondamentale memoria ([152]), Chevalley costruisce una teoria dell'intersezione per le varietà algebriche, piú generale di quella data alcuni anni prima da van der Waerden.[28] In particolare, viene sviluppata la teoria dei cosiddetti anelli locali "geometrici" (ossia degli anelli locali che intervengono in geometria algebrica) e si prova, tra l'altro, un notevole risultato, secondo cui "ogni dominio locale geometrico è analiticamente non ramificato, ossia è tale che il suo completamento è un anello ridotto".[29]

Il lavoro piú importante di Cohen, un allievo di Zariski, è dedicato allo studio degli anelli locali noetheriani completi, con particolare riguardo al caso degli anelli locali regolari (cfr. [154]). Il teorema principale afferma che "ogni anello locale completo è omomorfo ad un anello locale regolare completo, ossia, all'anello delle serie di potenze formali in un certo numero di variabili, a coefficienti in un campo oppure in un opportuno anello di valutazione".[30] Inoltre, in tale lavoro vengono dimostrati numerosi altri risultati, tra cui i seguenti:

i) l'anello delle serie di potenze formali $K[[X_1, \ldots, X_n]]$, a coefficienti in un campo K, è un UFD;

[26] In tale lavoro si definisce anello locale un anello noetheriano A con un unico ideale massimale $\mathfrak{m}$, tale che A contiene un campo K con la proprietà che $A/\mathfrak{m}$ è un K-modulo finito.

[27] E precisamente dei completamenti degli anelli locali ottenuti localizzando l'anello in questione rispetto ai suoi ideali massimali.

[28] La teoria di Chevalley sarà poi generalizzata da A. Weil in [126].

[29] Ciò non è vero per un dominio locale arbitrario; per una caratterizzazione dei domini locali con tale proprietà, si veda [224].

[30] Si noti che nella dimostrazione data da Cohen, il caso in cui l'anello locale in questione e il suo campo residuo hanno la stessa caratteristica (caso *equicaratteristico*) è nettamente distinto dal caso in cui le caratteristiche sono differenti.

ii) il "teorema della purezza" di Macaulay continua a valere per un qualsiasi anello locale regolare (equicaratteristico).

Conviene segnalare anche il lavoro [155] in cui si prova, tra l'altro, che "un anello è noetheriano, se e soltanto se, ogni ideale primo è finitamente generato"[31] e in particolare che "un dominio noetheriano locale ha dimensione 1, se e soltanto se, esiste un estremo superiore per il numero dei generatori di tutti i suoi ideali".[32]

Per quanto riguarda i contributi di Samuel, occorre citare innanzitutto l'ampia memoria [228], dedicata alla nozione di molteplicità. Egli prova che, se A è un anello noetheriano e $\mathfrak{q}$ è un ideale $\mathfrak{p}$-primario, allora, per n abbastanza grande, la lunghezza della potenza simbolica $\mathfrak{q}^{(n)}$ è un polinomio in n, denotato con $P_{\mathfrak{q}}(n)$: in particolare, se A è locale con ideale massimale $\mathfrak{m}$, e $\mathfrak{q}$ è un ideale $\mathfrak{m}$-primario, allora il grado d del polinomio $P_{\mathfrak{q}}(n)$ è lo stesso per ogni $\mathfrak{q}$, sicché tale intero d prende il nome di *dimensione* di A. Si prova poi che l'intero d così definito è proprio la lunghezza minima di un sistema di parametri dell'anello locale, sicché la definizione di dimensione sopra introdotta coincide con quella data da Chevalley in [151] (in cui, a sua volta, Chevalley aveva dimostrato che la definizione di dimensione da lui data, coincideva con la dimensione di Krull, per un anello noetheriano locale arbitrario, ossia senza campo base). Inoltre, servendosi sempre del polinomio $P_{\mathfrak{q}}(n)$, Samuel dà una definizione di molteplicità di un ideale $\mathfrak{m}$-primario che generalizza la definizione di molteplicità data da Chevalley[33] ed estende altresí la teoria dell'intersezione data da Chevalley in [152], nonché quella data da Weil in [126].

Infine, occorre segnalare anche la monografia [229], che contiene un'esposizione sistematica delle principali tecniche algebriche utilizzate per lo studio locale su una varietà algebrica, nell'intorno di un suo punto o di una sua sottovarietà.

[31] Tale risultato non continua piú a valere, sostituendo nell'enunciato "primo" con "massimale"; per un controesempio esplicito, si veda: M. NAGATA, *Some studies on semi-local rings*, in "Nagoya Math. J.", *3*, 1951, pp. 23-30.

[32] Ne segue che, se A è un dominio noetheriano di dimensione > 2, allora non esiste un estremo superiore (finito) per il numero dei generatori degli ideali di A. In proposito, J. D. SALLY e W. V. VASCONCELOS hanno dimostrato ("J. Pure and Applied Alg.", *4*, 1974, pp. 319-336) che esistono anelli noetheriani di dim ≤ 2, per cui non esiste un estremo superiore per il numero dei generatori degli ideali *primi*, e inoltre che un siffatto estremo superiore esiste, se gli anelli in questione sono K-algebre finitamente generate di dim ≤ 2 (essendo K un campo).

[33] Nel senso che non è piú limitata agli ideali primari generati da sistemi di parametri.

3.

Alcuni legami tra algebra commutativa e algebra omologica

Ci proponiamo in questa sezione di esporre brevemente alcune nozioni e risultati fondamentali di algebra omologica, ciò che riuscirà molto utile nel seguito.

La dimensione proiettiva di un modulo

Def. 3.1. Si definisce *complesso di catene* di A-moduli (essendo A un anello) una successione di A-moduli e di omomorfismi di A-moduli del tipo:

$$K: \qquad \to X_{n+1} \xrightarrow{d_{n+1}} X_n \xrightarrow{d_n} X_{n-1} \to \qquad \text{con } n \in \mathbf{Z},$$

che verifica la condizione seguente: $d_n \circ d_{n+1} = 0$,[1] per ogni $n \in \mathbf{Z}$. In particolare, esso prende il nome di *complesso sinistro*, se $X_k = 0$, per ogni $k \leq -1$. Inoltre il modulo quoziente $\operatorname{Ker} d_n / \operatorname{Im} d_{n+1}$ prende il nome di *modulo di omologia di dimensione n* del complesso (di catene) K, e si denota brevemente con $H_n(K)$.[2]

Def. 3.2. Sia A un anello e M un A-modulo. Si definisce *risoluzione proiettiva* (risp. *risoluzione libera*) di M, un complesso sinistro di

[1] È subito visto che ciò equivale alla condizione seguente: $\operatorname{Im} d_{n+1} \subseteq \operatorname{Ker} d_n$.

[2] Ricordiamo che si definisce *complesso di cocatene* di A-moduli una successione del tipo:

$$K: \qquad \to X^{n-1} \xrightarrow{d^{n-1}} X^n \xrightarrow{d^n} X^{n+1} \to \dots, \qquad \text{con } n \in \mathbf{Z},$$

tale che $d^n \circ d^{n-1} = 0$, per ogni $n \in \mathbf{Z}$. In modo analogo si danno poi le definizioni di *complesso destro* e di *modulo di coomologia di dimensione n* di un complesso (di cocatene) K, $H^n(K)$.

A-moduli proiettivi[3] (risp. liberi):

$$K: \qquad \to P_{n+1} \xrightarrow{d_{n+1}} P_n \xrightarrow{d_n} P_{n-1} \to \qquad \to P_1 \xrightarrow{d_1} P_0 \to 0,$$

insieme ad un omomorfismo $\varepsilon : P_0 \to M$, tale che la successione:

$$\to P_{n+1} \to P_n \to P_{n-1} \to \ldots \to P_1 \to P_0 \xrightarrow{\varepsilon} M \to 0$$

è esatta. Talvolta si dice anche che $K \xrightarrow{\varepsilon} M \to 0$ è una risoluzione proiettiva (risp. libera) di M.

Si verifica facilmente (cfr. la successiva sezione 4) che "ogni A-modulo M possiede almeno una risoluzione libera, dunque proiettiva" e in particolare che "se A è noetheriano, ogni A-modulo M di tipo finito possiede una risoluzione libera formata da A-moduli di tipo finito". Siamo così in grado di dare la seguente:

Def. 3.3. Sia A un anello e M un A-modulo (non nullo). Si dice che M ha *dimensione proiettiva* o *dimensione omologica* n, se M possiede una risoluzione proiettiva di *lunghezza* n, diciamo:

$$0 \to P_n \to P_{n-1} \to \qquad \to P_1 \to P_0 \to M \to 0,$$

e non possiede risoluzioni proiettive di lunghezza minore.[4] Si scrive allora $\mathrm{pd}_A M = n$ o più semplicemente $\mathrm{pd}\, M = n$.[5]

Enunciamo ora alcune proprietà notevoli (cfr. [11], [52]):

Proposizione 3.4. *Sia A un anello noetheriano e M un A-modulo di tipo finito. Allora:*

i) $$\mathrm{pd}_A M = \sup_{\mathfrak{m} \in \mathrm{Max}(A)} \mathrm{pd}_{A_\mathfrak{m}} M_\mathfrak{m} = \sup_{\mathfrak{p} \in \mathrm{Spec}(A)} \mathrm{pd}_{A_\mathfrak{p}} M_\mathfrak{p}\text{[6]};$$

[3] Ricordiamo che un modulo proiettivo è un addendo diretto di un modulo libero: per altre caratterizzazioni, cfr. [7] oppure [63].

[4] Si definisce *lunghezza* di una risoluzione proiettiva K del tipo considerato nella Def. 3.2, il più piccolo intero $i \geqslant 0$ (se esiste) tale che $P_j = 0$ per ogni $j > i$. Se M non possiede risoluzioni proiettive di lunghezza finita, si dice che la dimensione proiettiva di M è ∞.

[5] È chiaro che $\mathrm{pd}\, M = 0 \Leftrightarrow M$ è un modulo proiettivo (non nullo). Se $M = 0$, si conviene talvolta di scrivere $\mathrm{pd}\, 0 = -1$.

[6] Dunque, nelle ipotesi attuali, lo studio della dimensione proiettiva è ricondotto a quello della dimensione proiettiva di un modulo su un anello locale.

ii) *la dimensione proiettiva* $\mathrm{pd}_A M$ *è il più piccolo intero* $n \geq -1$ (*se esiste*) *tale che* $\mathrm{Tor}_i^A(M, A/\mathfrak{m})$[7] $= 0$, *per ogni* $i > n$ *e per ogni ideale massi-*

[7] Richiamiamo rapidamente le definizioni e le prime proprietà dei Tor (funtori di *torsione*) e degli Ext (funtori di *estensione*) (cfr. [63], [66]):

Siano M, N due A-moduli, essendo A un anello arbitrario, e sia (K, ε) una risoluzione proiettiva di M, diciamo:

$$\to P_n \xrightarrow{d_n} P_{n-1} \to \quad \to P_1 \xrightarrow{d_1} P_0 \xrightarrow{\varepsilon} M \to 0.$$

(I) Consideriamo il complesso sinistro:

$$K \otimes_A N: \qquad \to P_n \otimes_A N \to P_{n-1} \otimes_A N \to \qquad \to P_0 \otimes_A N \to M \otimes_A N \to 0$$

e poniamo, per definizione:

$$\mathrm{Tor}_0^A(M, N) = M \otimes_A N$$

$$\mathrm{Tor}_n^A(M, N) = H_n(K \otimes_A N) = \mathrm{Ker}\, d_n \otimes 1/\mathrm{Im}\, d_{n+1} \otimes 1, \text{ per } n \geq 1.$$

Si prova, tra l'altro, che:

i) $\mathrm{Tor}_n^A(M, N)$, con $n \geq 1$, non dipende dalla risoluzione proiettiva scelta per M;

ii) $\mathrm{Tor}_n^A(M, N) = \mathrm{Tor}_n^A(N, M)$, per $n \geq 0$;

iii) ad ogni successione esatta corta di A-moduli: $0 \to M' \to M \to M'' \to 0$ è associata una successione esatta lunga, detta successione esatta di omologia dei Tor (fissato un arbitrario modulo N):

$$\begin{gathered}\to \mathrm{Tor}_n^A(M, N) \to \mathrm{Tor}_n^A(M'', N) \to \mathrm{Tor}_{n-1}^A(M', N) \to \\ \to \mathrm{Tor}_{n-1}^A(M, N) \to \qquad \to M \otimes_A N \to M'' \otimes_A N \to 0.\end{gathered}$$

Conviene sottolineare che, per mezzo dei Tor, è possibile dare delle semplici caratterizzazioni per la piattezza: cfr. ad es. [1, Cap. 2, Esercizi 24 e 26]; si noti inoltre che ogni modulo proiettivo è piatto, ma non viceversa, in generale.

(II) Consideriamo il complesso destro:

$$\begin{aligned}\mathrm{Hom}_A(K, N):\quad 0 \to \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(P_0, N) \xrightarrow{\delta^0} \\ \to \mathrm{Hom}_A(P_{n-1}, N) \xrightarrow{\delta^{n-1}} \mathrm{Hom}_A(P_n, N) \xrightarrow{\delta^n}\end{aligned}$$

e poniamo, per definizione:

$$\mathrm{Ext}_A^0(M, N) = \mathrm{Hom}_A(M, N)$$

$$\mathrm{Ext}_A^n(M, N) = H^n(\mathrm{Hom}_A(K, N)) = \mathrm{Ker}\, \delta^n/\mathrm{Im}\delta^{n-1}, \text{ per } n \geq 1.$$

Ebbene, si prova che i funtori Ext^n godono di proprietà, solo in parte simili a quelle sopra citate per i Tor. In particolare:

j) $\mathrm{Ext}_A^n(M, N)$, con $n \geq 1$, non dipende dalla risoluzione proiettiva scelta per M;

male $\mathfrak{m}$ *di* A[8]*;*

iii) *M è proiettivo* $\Leftrightarrow \mathrm{Ext}^1_A(M, N)$[9] $= 0$, *per ogni A-modulo di tipo finito N.*

Osservazione 3.5. Conviene notare esplicitamente che, con una definizione analoga alla Def. 3.2, ossia facendo intervenire complessi destri di moduli iniettivi,[10] si introduce la nozione di *risoluzione iniettiva* di un modulo e, a partire da essa, analogamente alla Def. 3.3, si definisce la *dimensione iniettiva*, $\mathrm{id}_A M$, di un A-modulo M (non nullo).

Alcuni esempi di complessi

Consideriamo ora alcuni esempi (tratti da: D. Buchsbaum, *Lectures on regular local rings*, Lect. Notes Math., *86*, pp. 13-32, Springer, Berlin 1969) i quali mostrano l'esistenza di legami alquanto profondi tra informazioni di natura omologica e talune proprietà algebriche.

Esempio 3.6. Sia A un anello e x un elemento (non nullo) di A. Consideriamo allora il complesso (di catene):

$$K(x): \qquad \to 0 \to 0 \to A \xrightarrow{x} A \to 0,$$

jj) in generale, $\mathrm{Ext}^n_A(M, N) \neq \mathrm{Ext}^n_A(N, M)$, per $n > 0$: ciò è dovuto a ragioni intrinseche legate alla covarianza e alla controvarianza dei funtori $\mathrm{Hom}_A(M, -)$ e $\mathrm{Hom}(-, N)$ rispettivamente;

jjj) ad ogni successione esatta corta di A-moduli: $0 \to T' \to T \to T'' \to 0$ sono associate due successioni esatte lunghe, dette successioni esatte di coomologia degli Ext (fissati ad arbitrio M e N):

$$\begin{aligned} 0 \to \mathrm{Hom}_A(T'', N) \to \mathrm{Hom}_A(T, N) \to \mathrm{Hom}_A(T', N) \to \\ \to \mathrm{Ext}^1_A(T'', N) \to \ldots \to \mathrm{Ext}^{n-1}_A(T', N) \to \mathrm{Ext}^n_A(T'', N) \to \ldots \end{aligned}$$

$$\begin{aligned} 0 \to \mathrm{Hom}_A(M, T') \to \mathrm{Hom}_A(M, T) \to \mathrm{Hom}_A(M, T'') \to \\ \to \mathrm{Ext}^1_A(M, T') \to \ldots \to \mathrm{Ext}^{n-1}_A(M, T'') \to \mathrm{Ext}^n_A(M, T') \to \end{aligned}$$

[8] Si prova in generale (cfr. [59, p. 110, Prop. 2.1]) che "la dimensione proiettiva di un A-modulo M, essendo A un anello arbitrario, è il più piccolo intero $n > -1$ (se esiste) tale che $\mathrm{Ext}^i_A(M, N) = 0$, per ogni $i > n$ e per ogni A-modulo N".

[9] Cfr. nota 7.

[10] Ricordiamo che un modulo M si dice *iniettivo*, se per ogni successione esatta corta: $0 \to N' \to N \to N'' \to 0$, la successione associata (cfr. [1, Prop. 2.8]) $0 \to \mathrm{Hom}(N'', M) \to \mathrm{Hom}(N, M) \to \mathrm{Hom}(N', M) \to 0$ risulta esatta.

dove il simbolo x denota la moltiplicazione per l'elemento x. Si verifica subito che $H_0(K(x)) = A/(x)$ e $H_1(K(x)) = \{a \in A / ax = 0\} = \mathrm{Ann}\,(x)$: dunque H_0 "misura" l'invertibilità di x, mentre H_1 "misura" la proprietà di essere un divisore dello zero in A.[11]

Esempio 3.7. Sia A un anello e siano x, y elementi (non entrambi nulli) di A. Consideriamo allora il complesso (di catene):

$$K(x, y): \qquad \to 0 \to 0 \to A \xrightarrow{f} A \oplus A \xrightarrow{g} A \to 0\,,$$

dove f e g sono definiti ponendo rispettivamente:

$$f(a) = (-ay, ax)\,, \qquad g(a_1, a_2) = a_1 x + a_2 y\,.^{12}$$

Si ha:

$$H_0(K(x, y)) = A/(x, y)\,,$$
$$H_1(K(x, y)) = \{(a_1, a_2) \in A \oplus A / a_1 x + a_2 y = 0\} / \{(-ay, ax)\}\,,$$
$$H_2(K(x, y)) = \{a \in A / ax = ay = 0\} = \mathrm{Ann}\,((x, y))\,.$$

Ne segue in particolare che:

i) se x e y non sono entrambi divisori dello zero, allora $H_2 = 0$;

ii) se A è un dominio di integrità, si ha: $H_2 = 0$ e inoltre $H_1(K(x, y)) = (x : y)/(x)$[13];

iii) se per di piú, A è un UFD, si ha che x e y sono relativamente primi $\Leftrightarrow H_1 = 0$.

A questo punto, si potrebbe procedere ancora con la costruzione

[11] In modo analogo si studia il complesso $\to 0 \to 0 \to M \xrightarrow{x} M \to 0$, dove M è un A-modulo e x denota l'endomorfismo $m \mapsto xm$ di M ($m \in M$).

[12] Tale esempio generalizza in modo naturale l'esempio precedente: infatti, esso può essere ottenuto a partire dalla applicazione tra complessi $K(x) \xrightarrow{y} K(x)$, indotta dalla moltiplicazione per y:

$$\begin{array}{ccccccccc} \to 0 & \to & 0 & \to & A & \xrightarrow{x} & A & \to & 0 \\ & & & & {\scriptstyle y}\downarrow & & \downarrow{\scriptstyle y} & & \\ \to 0 & \to & 0 & \to & A & \xrightarrow{x} & A & \to & 0 \end{array}$$

e considerando poi il cosiddetto "mapping cone" associato ad essa (cfr., ad es. [63, p. 55]).

[13] Infatti, nell'omomorfismo canonico di proiezione $A \oplus A \to A$ dato da $(a_1, a_2) \mapsto a_2$, il modulo $\{(a_1, a_2)/a_1 x + a_2 y = 0\}$ risulta isomorfo all'ideale $(x : y)$ e in particolare il sottomodulo $\{(-ay, ax)\}$ ha come immagine l'ideale (x).

sopra sviluppata, considerando complessi, diciamo $K(x, y, z, \ldots)$; tuttavia è piú conveniente ricorrere alla seguente costruzione generale, che definisce il cosiddetto *complesso di Koszul* o complesso dell'algebra esterna:

Esempio 3.8. Sia $f : M \to A$ un omomorfismo di A-moduli, essendo A un anello arbitrario. Consideriamo allora il complesso (di catene):

$$K(f): \quad \to \overset{p}{\wedge} M \to \overset{p-1}{\wedge} M \to \quad \to \overset{2}{\wedge} M \to M \to 0,$$

dove $\overset{p}{\wedge} M$ denota la potenza esterna p-esima del modulo M[14] e gli omomorfismi, diciamo per brevità, $df : \overset{p}{\wedge} M \to \overset{p-1}{\wedge} M$ sono definiti ponendo:

$$df(m_1 \wedge \quad \wedge m_p) = \sum_i (-1)^{i+1} f(m_i) m_1 \wedge \quad \wedge \hat{m}_i \wedge \quad \wedge m_p,$$

dove la notazione $\hat{m}_i$ sta a significare che l'elemento m_i viene omesso (nel prodotto).

È subito visto che $df^2 = 0$, sicché si tratta di fatto di un complesso (di catene).

Ebbene, il complesso di Koszul possiede notevoli proprietà (cfr. [11], [52], [225]), e su ciò ritorneremo nel seguito. Ci limitiamo qui a segnalare una forma particolarmente interessante di tale complesso, nel caso in cui, partendo da una successione $x_1, \ldots, x_r$ di elementi di A, si considera l'omomorfismo di A-moduli $f: A^r \to A$ definito ponendo:

$$f(1, 0, \ldots, 0) = x_1, \; f(0, 1, 0, \ldots, 0) = x_2, \; \ldots, \; f(0, \ldots, 0, 1) = x_r;$$

in tal caso, il complesso $K(f)$ si denota piú semplicemente con $K(x_1, \ldots, x_r)$, o meglio con $K(x_1, \ldots, x_r, A)$.

Il grado di un modulo

Introduciamo innanzitutto una nozione semplice, ma estremamente importante, come si vedrà nel seguito:

[14] Ricordiamo (cfr. [10]) che, per definizione: $\overset{p}{\wedge} M = T^p(M)/\mathfrak{a}_p$, dove $T^p(M)$ denota il prodotto $M \otimes M \otimes \ldots \otimes M$ (p volte) e $\mathfrak{a}_p$ è il sottomodulo di $T^p(M)$ generato da tutti gli elementi del tipo: $x_1 \otimes \ldots \otimes x_p$, dove $x_i = x_j$ per qualche $i \neq j$; l'immagine di un elemento $x_1 \otimes \ldots \otimes x_p$ di $T^p(M)$ si denota con $x_1 \wedge \wedge \ldots \wedge x_p$. Per una trattazione ampia e dettagliata dell'algebra esterna (di un modulo) cfr. [4, Cap. 3].

Def. 3.9. Sia A un anello, M un A-modulo e sia $x_1, \ldots, x_n$ una successione di elementi di A. Si dice che $x_1, \ldots, x_n$ è una *M-successione* o una *successione M-regolare,*[15] se soddisfa alle seguenti condizioni:

(1) $(x_1, \ldots, x_n) M \neq M$;

(2) per ogni $i = 0, 1, \quad , n-1$, x_{i+1} non è un divisore dello zero su $M/(x_1, \ldots, x_i)M$, o in modo equivalente: $(x_1, \ldots, x_i)M : (x_{i+1}) = (x_1, \ldots, x_i)M$.[16]

Osservazione 3.10. (a) Si noti che gli elementi di una A-successione (dunque $M = A$) possono essere assimilati, in un certo senso, a delle variabili indipendenti. Per es., se $A = R[X_1, \quad , X_n]$ è l'anello dei polinomi in n indeterminate a coefficienti in un anello R, allora gli elementi $X_1, \ldots, X_n$ costituiscono chiaramente una A-successione. Viceversa, se A è un anello contenente un campo k, e se $x_1, \ldots, x_n$ formano una A-successione, allora gli elementi $x_i (1 \leq i \leq n)$ sono algebricamente indipendenti su k (cfr., ad es., I. Kaplansky, "Nagoya Math. J.", *20*, 1962, pp. 195-199).

(b) Si verifica facilmente che, se A è un dominio di integrità e $a, b \in A$, allora le seguenti condizioni sono tra loro equivalenti:

(1) a, b è una A-successione;

(2) l'ideale $(a + bX)$ nell'anello di polinomi $A[X]$ è primo.

Si ha così un altro esempio di legami che intercorrono tra proprietà omologiche e proprietà algebriche.

(c) La nozione di M-successione dipende, in generale, dall'ordine in cui vengono considerati gli elementi.[17] Tuttavia si dimostra, tra l'altro, che (cfr. [11, p. 102, Th. 28]) "se A è un anello noetheriano locale e M è un A-modulo finitamente generato, una successione $x_1, \ldots, x_n$ di elementi di A è M-regolare, se e soltanto se, tali risultano tutte le successioni ottenute da essa, mediante una permutazione arbitraria su n oggetti". Ebbene, vale anche un risultato inverso (ma solo in parte, cfr. [6]): "se un anello noetheriano A possiede una A-successione di lunghezza 3 e se in A ogni permutazione di una A-successione è una A-successione, allora A è locale".

[15] Se $M = A$, si parla anche semplicemente di "successione regolare".

[16] Si pone, per convenzione: $x_0 = 0$. Si noti che la condizione (1) è introdotta soltanto per comodità tecnica, con lo scopo di escludere essenzialmente gli elementi invertibili.

[17] Per es. si verifica facilmente che se $A = K[X, Y, Z]$, essendo K un campo arbitrario, allora la successione $X, Y(1-X), Z(1-X)$ è regolare, mentre la successione $Y(1-X), Z(1-X), X$ non lo è.

(d) Si prova senza difficoltà che "se $x_1, \dots, x_n$ è una M-successione (essendo M un modulo su un anello A arbitrario), allora gli ideali $(x_1), (x_1, x_2), \dots, (x_1, x_2, \dots, x_n)$ formano una catena ascendente in senso stretto". In particolare, se $x_1, \dots, x_n$ è una successione regolare in un anello noetheriano, si ha:

$$0 < \mathrm{ht}\,(x_1) < \mathrm{ht}\,(x_1, x_2) < \qquad < \mathrm{ht}\,(x_1, \dots, x_n),$$ [18]

sicché $n \leqslant \mathrm{ht}\,(x_1, \dots, x_n)$.

Dall'Osservazione 3.10 (d) segue che, se A è noetheriano e M è un A-modulo (non nullo), allora esistono sempre M-successioni *massimali*.[19] Vale in proposito il risultato generale seguente (cfr. [6]) il quale, a sua volta, suggerisce la successiva Def. 3.12:

Teorema 3.11. *Sia A un anello noetheriano, $\mathfrak{a}$ un ideale di A e M un A-modulo finitamente generato, e supponiamo che $\mathfrak{a}M \neq M$. Allora due M-successioni massimali arbitrarie contenute in $\mathfrak{a}$ hanno la medesima lunghezza.*

Def. 3.12. Sia A un anello noetheriano, $\mathfrak{a}$ un ideale di A e M un A-modulo di tipo finito con $\mathfrak{a}M \neq M$. Allora la comune lunghezza di tutte le M-successioni massimali in $\mathfrak{a}$ prende il nome di *grado di $\mathfrak{a}$ su M* e si denota con $\mathrm{gr}_A(\mathfrak{a}, M)$ o piú semplicemente con $\mathrm{gr}\,(\mathfrak{a}, M)$. In particolare, se $M = A$, si preferisce scrivere $\mathrm{gr}\,\mathfrak{a}$ in luogo di $\mathrm{gr}\,(\mathfrak{a}, A)$.[20]

Osservazione 3.13. Se A è un anello noetheriano locale e $\mathfrak{m}$ è il suo ideale massimale, allora il grado di $\mathfrak{m}$ su un A-modulo M si denota semplicemente con $\mathrm{gr}\,M$, in luogo di $\mathrm{gr}\,(\mathfrak{m}, M)$. Tuttavia, se $\mathfrak{a}$ è un ideale di A, la notazione $\mathrm{gr}\,\mathfrak{a}$ risulta ambigua, giacché può indicare sia $\mathrm{gr}\,(\mathfrak{a}, A)$ che $\mathrm{gr}\,(\mathfrak{m}, \mathfrak{a})$, ma ciò dovrebbe essere chiarito dal contesto.

[18] Ciò segue dalla Def. 3.9 (cfr. [1, Lemma 4.4, Teor. 7.13]), essendo l'altezza di un ideale $\mathfrak{a}$ (in un anello A arbitrario) definita da: $\mathrm{ht}\,\mathfrak{a} = \inf_{\mathfrak{p} \supseteq \mathfrak{a}} \mathrm{ht}\,\mathfrak{p}\,(\mathfrak{p} \in \mathrm{Spec}(A))$.

[19] Una M-successione $x_1, \dots, x_n$ si dice massimale, se non esiste alcun elemento $y \in A$ tale che $x_1, \dots, x_n, y$ è una M-successione.

[20] Il termine "grado" ora introdotto è dovuto a D. Rees [223]; tuttavia, taluni autori (per es. [11]) preferiscono parlare di $\mathfrak{a}$-profondità di M, denotata con $\mathrm{depth}_{\mathfrak{a}}(M)$, in luogo di grado di $\mathfrak{a}$ su M (si è scelto qui di usare il termine grado, anche perché la profondità è stata già introdotta in [1], in un altro contesto).

Segnaliamo che (cfr. [11, (15.B)]), nelle ipotesi della Def. 3.12, il grado di $\mathfrak{a}$ su M, $\mathrm{gr}(\mathfrak{a}, M)$ può essere caratterizzato anche come il piú piccolo intero n tale che $\mathrm{Ext}^n_A(A/\mathfrak{a}, M) \neq 0$. Nel caso non noetheriano, una teoria del grado è stata introdotta da S. F. Barger ("Proc. Amer. Math. Soc.", *36*, 1972, pp. 365-368) e ripresa poi da M. Hochster ("Proc. London Math. Soc.", *29*, 1974, pp. 55-76).

Raccogliamo ora in un unico risultato alcune proprietà notevoli del grado (cfr. [6; Th. 125, Th. 129], [11, (15.G)]):

Teorema 3.14. *Sia A un anello noetheriano, $\mathfrak{a}$ un ideale proprio di A e M un A-modulo di tipo finito. Allora:*

(1) $\operatorname{gr}(\mathfrak{a}, M) = \inf_{\mathfrak{p} \supseteq \mathfrak{a}} \operatorname{gr} M_{\mathfrak{p}}$ $(\mathfrak{p} \in \operatorname{Spec}(A))$;

(2) *se $\mathfrak{a}$ è generato da n elementi, allora $\operatorname{gr} \mathfrak{a} \leqslant n$; se in particolare $\operatorname{gr} \mathfrak{a} = n$, allora $\mathfrak{a}$ può essere generato da n elementi che formano una A-successione;*

(3) *se per di più A è locale e $\mathfrak{a} = (x_1, \ldots, x_n)$, allora $\operatorname{gr} \mathfrak{a} = n$ se, e soltanto se, gli elementi $x_1, \ldots, x_n$ formano una A-successione.*

Alcuni risultati generali

Cominciamo col dare un primo risultato, dovuto a Rees, che collega le nozioni di grado e di dimensione proiettiva (cfr. [223]):

Teorema 3.15. *Sia A un anello noetheriano, M un A-modulo di tipo finito non nullo e sia $\mathfrak{a} = \operatorname{Ann}(M)$. Allora si ha:*

$$\operatorname{gr} \mathfrak{a} \leqslant \operatorname{pd}_A M.$$

Def. 3.16. Sia M un modulo di tipo finito non nullo su un anello noetheriano A e sia $\mathfrak{a} = \operatorname{Ann}(M)$. Allora M si dice *perfetto*, se $\operatorname{gr} \mathfrak{a} = \operatorname{pd}_A M$. Inoltre un ideale $\mathfrak{b}$ di A si dice *perfetto*, se $A/\mathfrak{b}$ è un A-modulo perfetto, ossia, se $\operatorname{gr} \mathfrak{b} = \operatorname{pd}_A(A/\mathfrak{b})$.

Osservazione 3.17. Conviene sottolineare che la definizione di ideale perfetto coincide, nel caso geometrico, ossia per un ideale omogeneo nell'anello dei polinomi $k[X_0, \ldots, X_n]$ (essendo k un campo), con una classica definizione di Macaulay (cfr. [98]). Tra gli esempi di ideali perfetti, ricordiamo in particolare[21]:

(a) gli ideali generati da una A-successione, insieme a tutte le loro potenze (cfr. [223] e [6, p. 127]);

(b) gli ideali $I_t(x_{ij})$ generati dai (determinanti dei) minori di ordine t di una matrice $r \times s$ di indeterminate sopra un campo k nell'anello $k[x_{ij}]_{\substack{i=1,\ldots,r\\ j=1,\ldots,s}}$, per ogni t tale che $1 \leqslant t \leqslant \min\{r, s\}$ (cfr. [29]).

[21] Vedremo nella sezione 4 un esempio di ideale primo omogeneo, in un anello di polinomi, non perfetto.

Un altro risultato fondamentale che collega il grado con la dimensione proiettiva è dato dal teorema seguente, dovuto ad Auslander e Buchsbaum:

Teorema 3.18. *Sia A un anello locale noetheriano e sia M un A-modulo di tipo finito non nullo tale che* $\mathrm{pd}_A M < \infty$. *Allora si ha:*

$$\mathrm{pd}_A M = \mathrm{gr}\, A - \mathrm{gr}\, M.$$ [22]

Il Teorema 3.18 è evidente, se M è proiettivo, nel qual caso $\mathrm{pd}_A M = 0$ e $\mathrm{gr}\, M = \mathrm{gr}\, A$, giacché $M \cong A^n$ (essendo A locale). È chiaro poi che, se $\mathrm{gr}\, A = 0$, ossia, se l'ideale massimale di A è costituito interamente da divisori dello zero, allora $\mathrm{pd}_A M = 0$.

Enunciamo infine un altro risultato generale (cfr. [11, (15.F)]):

Teorema 3.19. Sia A un anello locale noetheriano e sia M un A-modulo di tipo finito non nullo. Allora si ha: $\mathrm{gr}\, M \leqslant \dim M$.[23]

Osservazione 3.20. Dal teorema precedente segue subito che, nelle ipotesi ivi enunciate, si ha sempre: $\mathrm{gr}\, M < \infty$; ebbene, in virtù del Teorema 3.14(1); un risultato analogo continua a valere per un anello noetheriano qualsiasi.[24] Invece, se M è un modulo di tipo finito non nullo su un anello locale noetheriano A, non si verifica necessariamente che $\mathrm{pd}_A M < \infty$[25] (come apparirà chiaro alla fine delle sezione).

Anelli di Cohen-Macaulay e anelli di Gorenstein

Diamo innanzitutto una prima definizione (cfr. Teor. 3.19):

Def. 3.21. Sia A un anello locale noetheriano e M un A-modulo di tipo finito. Allora si dice che M è un *modulo di Cohen-Macaulay*,

[22] Conviene segnalare fin d'ora che, se A è un anello locale regolare (o più in generale, di Cohen-Macaulay) di $\dim n$, allora risulta: $\mathrm{gr}\, A = \dim A = n$, sicché la tesi si scrive: $\mathrm{pd}_A M = n - \mathrm{gr}\, M$. Ciò giustifica la denominazione di "codimensione omologica" introdotta originariamente da Auslander e Buchsbaum per indicare il grado $\mathrm{gr}\, M$ (usata anche in [52]).

[23] Ricordiamo che, se M è un modulo non nullo su un anello A arbitrario, si pone, per definizione, $\dim M = \dim A/\mathrm{Ann}\,(M)$.

[24] Ciò si prova anche direttamente, per altra via (cfr. [6, Th. 125]).

[25] Conviene segnalare in proposito un risultato alquanto interessante ottenuto da H. Bass e M. P. Murthy ("Ann. of Math.", *86*, 1967, pp. 16-73), che completa la Prop. 3.4(i), secondo cui "se M è un modulo finitamente generato su un anello noetheriano A tale che, per ogni ideale primo $\mathfrak{p}$ di A, si ha: $\mathrm{pd}_{A_\mathfrak{p}} M_\mathfrak{p} < \infty$, allora risulta: $\mathrm{pd}_A M < \infty$".

se ($M = 0$ oppure se) gr $M = \dim M$. In particolare, un anello locale noetheriano A si dice di Cohen-Macaulay, se tale risulta come A-modulo.

Si dimostra (cfr., ad es., [11, (16.D)]) che un anello locale noetheriano A è di Cohen-Macaulay, se e soltanto se, in A vale il *teorema della purezza*: "ogni ideale $\mathfrak{a}$ in A *di classe principale* (ossia generato da un numero di elementi uguale a ht $\mathfrak{a}$) è puro".[26] Ma allora, tenendo presente il carattere locale del teorema della purezza ([11, (16.C)]), si è condotti in modo naturale a dare la seguente definizione, che estende quella sopra data:

Def. 3.22. Un anello noetheriano A si dice un *anello di Cohen-Macaulay*, brevemente CM, se in A vale il teorema della purezza.

Sussiste il risultato seguente, di notevole importanza (cfr. [11]):

Teorema 3.23. *Le seguenti condizioni sono tra loro equivalenti, per un anello noetheriano A:*

(a) A è CM*;*

(b) *ogni ideale di A generato da una A-successione è puro;*

(c) gr $\mathfrak{a}$ = ht $\mathfrak{a}$ *per ogni ideale* $\mathfrak{a}$ *di* A[27]*;*

(d) $A_{\mathfrak{p}}$ *è* CM *per ogni ideale primo* $\mathfrak{p}$ *di* A*;*

(e) $A_{\mathfrak{m}}$ *è* CM *per ogni ideale massimale* $\mathfrak{m}$ *di* A.

Osservazione 3.24. (a) Ogni dominio noetheriano A di dimensione 1 è CM: basta supporre A locale e osservare che ogni elemento non nullo dell'ideale massimale costituisce una successione regolare (stante la Def. 3.21). In modo analogo si prova che ogni dominio noetheriano integralmente chiuso di dimensione 2 è CM.[28] Inoltre ([15, vol. II, p. 397]) ogni anello locale regolare è CM.

(b) Gli anelli CM godono di molte buone proprietà, tra cui le classiche "proprietà di trasporto". Piú precisamente, si dimostra (cfr. [27]) che:

"Se A è un anello noetheriano e $X_1, \ldots, X_n$ sono indeterminate

[26] Ciò giustifica, alla luce delle considerazioni sviluppate nella sezione precedente, la denominazione assegnata a tali anelli. Si prova inoltre (cfr. [216], [223]) che in un anello siffatto ogni ideale perfetto è puro.

[27] Si noti che il grado gr $\mathfrak{a}$ rimpiazza in modo efficace l'altezza in molti problemi di carattere omologico, relativi ad anelli che non sono di Cohen-Macaulay.

[28] Ciò non è vero in generale: un esempio di dominio noetheriano integralmente chiuso di dimensione 3 che non è CM si trova costruito esplicitamente in [19, p. 149].

indipendenti su A, allora le seguenti condizioni sono tra loro equivalenti:

(1) A è CM;

(2) $A[X_1, \ldots, X_n]$ è CM;

(3) $A[[X_1, \ldots, X_n]]$ è CM."

(c) Particolare importanza hanno gli anelli quozienti di anelli CM: tali risultano, ad es., gli anelli delle coordinate di una varietà algebrica affine o proiettiva; è chiaro inoltre che non è restrittivo limitarsi a considerare il caso locale. In particolare, se A è un anello CM e $\mathfrak{a}$ è un ideale di classe principale in A, allora $A/\mathfrak{a}$ risulta un anello CM,[29] sicché l'anello delle coordinate di una varietà algebrica intersezione completa è di Cohen-Macaulay.

Passiamo ora a introdurre rapidamente una classe notevole di anelli CM: i cosiddetti anelli di Gorenstein.

Partiamo da un risultato, dovuto a Northcott e Rees (cfr. [25]):

Teorema 3.25. *Sia A un anello locale CM di dimensione d e siano $x_1, \ldots, x_d$ e $y_1, \ldots, y_d$ due sistemi di parametri per A. Allora, posto: $\mathfrak{a} = (x_1, \ldots, x_d)$ e $\mathfrak{b} = (y_1, \ldots, y_d)$, il numero delle componenti irriducibili che compaiono in una decomposizione irriducibile irridondante di $\mathfrak{a}$[30] è uguale al numero delle componenti irriducibili che compaiono in una decomposizione irriducibile irridondante di $\mathfrak{b}$.*[31]

Ne segue in particolare che ad ogni anello locale CM è possibile associare un invariante numerico, espresso da un intero $\geqslant 1$, che prende il nome di *indice di irriducibilità* di A. Ebbene, gli anelli locali CM per cui tale indice vale 1 prendono il nome di anelli di Gorenstein:

Def. 3.26. Sia A un anello locale CM. Si dice che A è un *anello di Gorenstein*, se esiste un sistema di parametri per A che genera un ideale irriducibile, ossia (3.25), se ogni sistema di parametri genera un ideale irriducibile.

[29] Basta ricondursi al caso locale, e utilizzare il Teor. 3.14(3) e un'osservazione elementare sui quozienti di moduli di Cohen-Macaulay [11, (16.A) (2)].

[30] Cfr. [1, Cap. 7, Esercizio 19].

[31] Tale risultato estende largamente un'osservazione di Gröbner (1934), in base alla quale "se A è un anello locale regolare di dimensione d e se $x_1, \ldots, x_d$ è un sistema di parametri per A, allora l'ideale $(x_1, \ldots, x_d)$ è irriducibile". Segnaliamo inoltre che il Teor. 3.25 non si inverte, ossia non è possibile caratterizzare gli anelli locali CM mediante la proprietà ivi enunciata (a tale proposito, cfr. [25]).

Vale il seguente risultato (cfr. [141]):

Teorema 3.27 *Le seguenti condizioni sono tra loro equivalenti per un anello noetheriano A arbitrario:*

(a) *$A_{\mathfrak{p}}$ è di Gorenstein, per ogni ideale primo $\mathfrak{p}$ di A;*

(b) *$A_{\mathfrak{m}}$ è di Gorenstein, per ogni ideale massimale $\mathfrak{m}$ di A;*

(c) *ogni ideale di classe principale in A è puro e le sue componenti primarie sono irriducibili.*

Osservazione 3.28. (a) In virtú del Teorema 3.27, un anello noetheriano A si dice un *anello di Gorenstein*,[32] se soddisfa ad una qualsiasi delle condizioni ivi enunciate. Occorre sottolineare inoltre che ci siamo limitati qui, per semplicità, a introdurre tale classe di anelli in un contesto puramente algebrico: una trattazione organica e sviluppata da vari punti di vista, ivi incluso un approccio omologico,[33] si trova nella fondamentale memoria di H. Bass [141].

(b) Tra gli esempi di anelli (locali) di Gorenstein, segnaliamo gli anelli locali regolari (cfr. 3.24 (a)), gli anelli del tipo $A/(x_1, \ldots, x_n)$, dove A è un anello locale regolare e $x_1, \ldots, x_n$ è una A-successione[34] e i quozienti di anelli locali regolari che sono per di piú CM e UFD, in virtú di un classico risultato di M. P. Murthy [206].

(c) Si noti che l'enunciato riportato nell'Oss. 3.24 (b) continua a valere anche sostituendo ovunque "CM" con "Gorenstein" (cfr. [27]).

(d) Segnaliamo alcuni esempi di anelli CM *non* di Gorenstein, dati da J. Eagon ("Math. Z.", *109*, 1969, pp. 109-111) e da M. Fiorentini ("Rend. Acc. Naz. Lincei", *50*, 1971, pp. 54-59 e 244-249).

[32] Tale denominazione è dovuta ad un classico risultato di Gorenstein, secondo cui "se Q è un punto di una curva piana, allora posto: $\delta_Q = \dim \bar{O}_Q/O_Q$ e $n_Q = \dim \bar{O}_Q/\mathfrak{c}_Q$, essendo $\mathfrak{c}_Q$ il conduttore ([15, vol. 1]), si ha: $n_Q = 2\delta_Q$". Ebbene tale proprietà, ottenuta da Gorenstein in relazione ad una caratterizzazione delle curve aggiunte ad una curva piana irriducibile assegnata ("Trans. Amer. Math. Soc.", *72*, 1952, pp. 414-436), è stata il punto di partenza di numerose ricerche nell'ambito della geometria algebrica, ad opera soprattutto di Rosenlicht, Grothendieck e Serre ([122], [235]) ed è stata infine "assiomatizzata" da Bass in [141].

[33] Si dimostra, tra l'altro, che un anello locale noetheriano A è di Gorenstein $\Leftrightarrow \mathrm{id}_A A < \infty$ ($\Leftrightarrow \mathrm{id}_A A = \dim A$), dove il simbolo id denota la dimensione iniettiva (3.5): cfr. [141], [6], [25].

[34] Chiamati anche "intersezioni complete", per il loro significato geometrico.

Anelli locali regolari

Sia A un anello locale regolare e $\mathfrak{m}$ il suo ideale massimale: è noto che A è un dominio integralmente chiuso ([1, Lemma 11.23] e [11, (17.F)]) di Cohen-Macaulay e per di piú di Gorenstein, in virtú dell'Oss. 3.28 (b).

Tra gli esempi piú significativi di tali anelli ricordiamo l'anello locale di una varietà algebrica in un suo punto semplice, gli anelli delle serie di potenze formali sopra un campo e gli anelli delle serie di potenze convergenti sul campo complesso.

Osserviamo poi che ha interesse sapere quando un quoziente di un anello locale regolare è ancora un anello locale regolare, giacché tale situazione si presenta spontaneamente in vari contesti: infatti, possono essere espressi come quozienti di anelli locali regolari, tra gli altri, gli anelli locali delle varietà algebriche, gli anelli locali di funzioni analitiche e gli anelli locali completi (in virtú dei teoremi di Cohen, a cui si è accennato nella sezione precedente). Ebbene, vale in proposito un classico risultato di Chevalley [12, (25.18)]:

Proposizione 3.29. *Sia A un anello locale regolare e $\mathfrak{a}$ un ideale di A. Allora le seguenti condizioni sono tra loro equivalenti:*

(a) *$A/\mathfrak{a}$ è un anello locale regolare;*

(b) *$\mathfrak{a}$ è generato da un sottoinsieme di un sistema regolare di parametri*[35] *per A.*

Passiamo ora a enunciare (cfr. [29]) il celebre Teorema di Auslander, Buchsbaum e Serre (il primo grosso successo dei nuovi metodi omologici), dimostrato intorno al 1955 da Auslander e Buchsbaum in [135][36] e indipendentemente da Serre in [234]:

Teorema 3.30. *Sia A un anello locale noetheriano, $\mathfrak{m}$ il suo ideale massimale e $k = A/\mathfrak{m}$ il suo campo residuo. Allora le seguenti condizioni sono tra loro equivalenti:*

(a) *A è regolare;*

[35] Si definisce sistema regolare di parametri, per un anello locale regolare, un sistema minimale di generatori dell'ideale massimale; dunque (cfr. [11, (16.B)]) la (b) implica in particolare la condizione seguente: "$\mathfrak{a}$ è generato da una A-successione". Piú in generale, si prova (cfr. [223]) che "$A/\mathfrak{a}$ è un anello di Cohen-Macaulay se, e soltanto se, $\mathfrak{a}$ è un ideale perfetto".

[36] Una versione preliminare era stata annunciata in: M. Auslander, D. Buchsbaum, *Homological dimension in Noetherian rings*, in "Proc. Nat. Acad. Sci. USA", *42*, 1956, pp. 36-38.

(b) $\mathrm{pd}_A k < \infty$[37];

(c) *per ogni A-modulo M di tipo finito, si ha:* $\mathrm{pd}\, M < \infty$;

(d) *per ogni A-modulo M, si ha:* $\mathrm{pd}\, M \leqslant \dim A$.

Dal teorema precedente discendono in particolare due corollari notevoli (cfr. [11] o [29]), i quali risolvono completamente, in senso affermativo, due "congetture di Krull" enunciate nella sezione precedente:

Corollario 3.31. *Se A è un anello locale regolare e $\mathfrak{p}$ è un ideale primo arbitrario di A, allora $A_{\mathfrak{p}}$ è un anello locale regolare.*

Corollario 3.32. *Ogni anello locale regolare è un* UFD.

Osservazione 3.33. (a) Ricordiamo innanzitutto (cfr. [11]) che si definisce ***dimensione globale*** di un anello A arbitrario, il valore del sup $\mathrm{pd}_A M$, al variare di M nella classe di tutti gli A-moduli (tale valore può ben essere ∞), il quale si denota con $\mathrm{gl}\dim A$. Allora segue in particolare dal Teorema 3.30 che "un anello locale noetheriano A è regolare $\Leftrightarrow$[38] $\mathrm{gl}\dim A = \dim A$". A questo punto, tenendo presente (cfr. [11], [62]) che il famoso Teorema delle sizigie di Hilbert può enunciarsi anche dicendo che "se $A = k[X_1, \ldots, X_n]$ è l'anello dei polinomi in n indeterminate a coefficienti in un campo k arbitrario, allora $\mathrm{gl}\dim A = n$", si può affermare senz'altro che la validità del Teorema delle sizigie caratterizza gli anelli locali regolari.[39]

(b) Una prima "estensione" del Teorema 3.30 è dovuta a J. Tate [241]. In tale lavoro, si studiano anzitutto, nel caso in cui A è un anello locale noetheriano qualsiasi, $\mathfrak{m}$ il suo ideale massimale e k il suo campo residuo, i cosiddetti numeri di Betti $B_r(A) = \dim_k \mathrm{Tor}_r^A(k, k)$, e si dimostra, tra l'altro, che "se A non è regolare, si ha: $B_r(A) \geqslant \geqslant \binom{n}{r} + \binom{n}{r-2} + \ldots$, da cui: $B_r(A) \geqslant 2^{n-1}$ per $r \geqslant n$, dove n è il minimo numero di elementi che generano $\mathfrak{m}$"; si ottiene in tal modo

[37] Si ha allora (cfr. [31, p. 169, Th. 2]) che "A è locale regolare $\Leftrightarrow$ $\mathrm{pd}_A \mathfrak{m} < \infty$".

[38] E inoltre (cfr. [11, p. 130, Lemma 5 (II)]) che "un anello locale noetheriano è règolare $\Leftrightarrow$ la sua dimensione globale è finita". Conviene notare esplicitamente che l'unica implicazione realmente difficile è quella inversa ($\Leftarrow$): per una discussione in proposito, cfr. [11].

[39] Conviene segnalare che la teoria delle sizigie è stata ripresa sistematicamente soltanto nel 1949, da Gröbner [98], mentre la prima estensione, in senso "omologico", del Teorema delle sizigie è dovuta a H. Cartan ("Rend. Mat.", (5), *11*, 1952, pp. 156-166).

(cfr. [11, p. 130, Th. 41]) una nuova dimostrazione del fatto che ogni anello locale noetheriano di dimensione globale finita è regolare (e viceversa).[40] Nello stesso lavoro, Tate dimostra che, se A è un anello locale "intersezione completa", la serie di Poincaré di A, ossia la serie di potenze formale $P(A) = \sum_{r=0}^{\infty} B_r(A) z^r$ è una funzione razionale in z. Tale risultato era collegato ad una congettura di Kaplansky e Serre, secondo cui $P(A)$ è una funzione razionale, per un qualsiasi anello locale noetheriano A (una discussione di alcuni risultati parziali ottenuti in proposito, si trova in [61]). Ebbene, recentemente, D. Anick ha fornito un controesempio a tale congettura.

(c) Segnaliamo ancora una generalizzazione del Teorema 3.30 dovuta a W. V. Vasconcelos [245], secondo cui "un ideale $\mathfrak{a}$ di un anello locale noetheriano A è generato da una A-successione, se e soltanto se, pd $\mathfrak{a} < \infty$ e inoltre $\mathfrak{a}/\mathfrak{a}^2$ è un $A/\mathfrak{a}$-modulo libero".[41]

(d) Il Corollario 3.32 è stato dimostrato per la prima volta da M. Auslander e D. Buchsbaum in [137] ed è stato da allora oggetto di grande interesse: tale risultato è stato utilizzato in numerose questioni di algebra e di geometria (tra le quali, il problema della risoluzione delle singolarità risolto, in caratteristica zero, da H. Hironaka in [186]) e in particolare, sono state date di esso numerose dimostrazioni (cfr. [6]).

(e) Per finire, segnaliamo alcuni risultati alquanto espressivi riguardanti gli anelli locali regolari di caratteristica $p \neq 0$, ottenuti da E. Kunz ("Amer. J. Math.", *91*, 1969, pp. 772-784).

[40] Vedi nota 38.

[41] Vedi nota 37. Tale risultato è stato ottenuto indipendentemente da D. Ferrand ("C. R. Acad. Sci. Paris", *264*, 1967, pp. A427-A428) ed è stato generalizzato recentemente da M. Boratyński ("J. Algebra", *57*, 1979, pp. 236-241).

4.

Alcuni risultati e problemi riguardanti i metodi omologici in algebra commutativa

Ci proponiamo ora di sviluppare alcune nozioni introdotte nella sezione precedente, allo scopo di poter accennare ad alcuni risultati notevoli ottenuti negli ultimi anni da Buchsbaum e Eisenbud, nonché a taluni problemi aperti relativi alla teoria omologica dei moduli, di grande attualità e interesse.

Generalità sulle risoluzioni libere finite

Def. 4.1. Sia M un modulo di tipo finito su un anello noetheriano A. Allora una risoluzione libera di M, diciamo:

$$X: \quad \to F_i \xrightarrow{d_i} F_{i-1} \xrightarrow{d_{i-1}} F_{i-2} \to \quad \to F_1 \xrightarrow{d_1} F_0 \xrightarrow{\varepsilon} M \to 0,$$

si dice *finita*, se F_i ha rango finito, per ogni indice i, e inoltre $F_i = 0$ per $i \gg 0$. In tal caso, si dice brevemente che X è una FFR.

Tale nozione che, come si vedrà meglio nel seguito, è estremamente significativa, risale sostanzialmente a Hilbert: infatti, dal celebre Teorema delle sizigie, segue in particolare che "ogni modulo graduato[1] finitamente generato sull'anello di polinomi $K[X_1, \ldots, X_n]$, essendo K un campo, possiede una FFR"; occorre aggiungere inoltre che Hilbert fornì anche un algoritmo per trovare una siffatta FFR e

[1] Si noti che dal Teorema delle sizigie segue, più in generale, che ogni modulo di tipo finito (non necessariamente graduato) sull'anello $K[X_1, \ldots, X_n]$ possiede una risoluzione *proiettiva* finita e di lunghezza $\leqslant n$, sicché, in virtù del risultato di QUILLEN [221] e SUSLIN [238], ogni modulo di tipo finito su $K[X_1, \ldots, X_n]$ possiede una FFR.

provò che la lunghezza[2] di una tale risoluzione, supposta di lunghezza minimale, è al piú n (ossia, il numero delle variabili).

Facciamo vedere ora che, se A è un anello noetheriano e M è un A-modulo finitamente generato, allora M possiede una risoluzione libera formata da A-moduli liberi di tipo finito (ma non necessariamente una FFR).

Cominciamo con l'osservare che (cfr. [1, Prop. 2.3]) assegnare un sistema di generatori, diciamo $x_1, \ldots, x_{n_0}$ per M equivale ad assegnare un omomorfismo di A-moduli da un modulo libero A^{n_0} su M, definito associando ad un elemento $(r_1, \ldots, r_{n_0})$ di A^{n_0} l'elemento $\sum_{i=1}^{n_0} r_i x_i$ di M. Dunque lo studio del modulo M è ricondotto all'esame del nucleo di tale omomorfismo, ossia del sottomodulo $\{(r_1, \ldots, r_{n_0}) \in A^{n_0} / \sum_i r_i x_i = 0\}$, il quale prende il nome di (*primo*) *modulo di sizigie* per M e si denota con $\operatorname{syz}^1 M$.[3] Ora, a partire da $\operatorname{syz}^1 M$, il quale è ancora un A-modulo finitamente generato, si può ripetere una costruzione simile a quella sopra fatta per M, sicché, scelti n_1 generatori, diciamo, per $\operatorname{syz}^1 M$, si ottiene un modulo di sizigie per $\operatorname{syz}^1 M$, che si denota con $\operatorname{syz}^2 M$. Ripetendo ancora la costruzione e proseguendo in tal modo, si ottiene una successione (eventualmente infinita) di moduli di sizigie, $\operatorname{syz}^i M$, ciascuno contenuto in un modulo libero A^{n_i}, che per semplicità denoteremo con F_i:

$$\to F_3 \twoheadrightarrow \operatorname{syz}^3 M \hookrightarrow F_2 \twoheadrightarrow \operatorname{syz}^2 M \hookrightarrow F_1 \twoheadrightarrow \operatorname{syz}^1 M \hookrightarrow F_0 \to M \to 0,$$

a partire dalla quale, denotando con d_i l'omomorfismo composto: $F_i \twoheadrightarrow \operatorname{syz}^i M \hookrightarrow F_{i-1}$, per ogni i, si ottiene una successione esatta:

$$\to F_i \xrightarrow{d_i} F_{i-1} \xrightarrow{d_{i-1}} F_{i-2} \to \qquad \to F_1 \xrightarrow{d_1} F_0 \to M \to 0,$$

la quale è proprio una risoluzione libera del tipo cercato.[4]

Passiamo ora a considerare, su due esempi geometrici (essendo k un campo algebricamente chiuso), la successione dei moduli di sizigie:

[2] Vedi la nota 4 della sezione precedente.

[3] È chiaro che $\operatorname{syz}^1 M$ non è univocamente determinato, poiché dipende dalla scelta dei generatori per M.

[4] In particolare, abbiamo dimostrato che ogni modulo di tipo finito M su un anello noetheriano A è *di presentazione finita*, ossia possiede una successione esatta della forma: $A^m \to A^n \to M \to 0$, con m, n interi ≥ 1. È chiaro poi che, con un'argomentazione simile a quella sviluppata, si prova che ogni modulo su un anello arbitrario possiede una risoluzione libera.

Esempio 4.2. Sia $A = k[X_0, X_1, X_2, X_3]$ e $M = \mathfrak{a} = (X_1X_3 - X_2^2, X_1X_2 - X_0X_3, X_0X_2 - X_1^2)$, sicché $\mathfrak{a}$ è l'ideale primo associato alla cubica sghemba di $\mathbf{P}^3_k$ [101, p. 21].

Ebbene una sizigia di $\mathfrak{a}$ è data da una terna di elementi di A, diciamo (f_1, f_2, f_3) tale che: $f_1(X_1X_3 - X_2^2) + f_2(X_1X_2 - X_0X_3) + f_3(X_0X_2 - X_1^2) = 0$, da cui, in particolare:

$$\begin{aligned} f_1 &\in (X_1X_2 - X_0X_3, X_0X_2 - X_1^2) : (X_1X_3 - X_2^2) = \\ &= [(X_0, X_1) \cap \mathfrak{a}]^5 : (X_1X_3 - X_2^2) = \\ &= [(X_0, X_1) : (X_1X_3 - X_2^2)] \cap [\mathfrak{a} : (X_1X_3 - X_2^2)] = (X_0, X_1); \end{aligned}$$

in modo analogo, si ottiene che $f_2 \in (X_1, X_2)$ e $f_3 \in (X_2, X_3)$. Più precisamente, si prova che:

$$(f_1, f_2, f_3) \in \operatorname{syz}^1\mathfrak{a} \Leftrightarrow (f_1, f_2, f_3) = \alpha(X_0, X_1, X_2) + \beta(X_1, X_2, X_3)$$

con $\alpha, \beta \in A$.

Ora, le terne (X_0, X_1, X_2) e (X_1, X_2, X_3) sono linearmente indipendenti su A, com'è subito visto, sicché $\operatorname{syz}^1\mathfrak{a} \cong A^2$ e quindi $\mathfrak{a}$ possiede una risoluzione libera finita della forma:

$$0 \to \operatorname{syz}^1\mathfrak{a} \to A^3 \to \mathfrak{a} \to 0,$$

sicché $\operatorname{pd}_A A/\mathfrak{a} \leq 2$.[6]

D'altra parte, essendo A un anello CM, si ha (3.23): $\operatorname{gr} \mathfrak{a} = 2$ e quindi, in virtú di 3.15, si conclude che $\mathfrak{a}$ è un ideale perfetto, o come si dice anche, che la cubica sghemba di $\mathbf{P}^3$ è una varietà perfetta.[7]

Esempio 4.3. Sia $A = k[X_0, X_1, X_2, X_3]$ e $M = \mathfrak{a} = (X_0^2X_2 - X_1^3, X_0X_3 - X_1X_2, X_0X_2^2 - X_1^2X_3, X_1X_3^2 - X_2^3)$, sicché $\mathfrak{a}$ è l'ideale primo associato alla quartica di II specie di $\mathbf{P}^3_k$ (cfr. [98]).

In tal caso, è subito visto che le seguenti quaterne (ordinate) di elementi di A:

$$\begin{aligned} &\alpha_1 = (X_2, -X_1^2, -X_0, 0), \ \alpha_2 = (X_3, -X_0X_2, -X_1, 0), \\ &\alpha_3 = (0, X_1X_3, -X_2, -X_0), \ \alpha_4 = (0, X_2^2, -X_3, -X_1) \end{aligned}$$

[5] Infatti, la quartica di I specie di $\mathbf{P}^3$, intersezione delle quadriche di eq. $X_1X_2 - X_0X_3 = 0$ e $X_0X_2 - X_1^2 = 0$, è spezzata in due componenti irriducibili, date dalla cubica in questione e dalla retta di eq. $X_0 = X_1 = 0$.

[6] Basta considerare la risoluzione libera: $0 \to \operatorname{syz}^1\mathfrak{a} \to A^3 \to A \to A/\mathfrak{a} \to 0$

[7] Ci limitiamo qui a segnalare, tra le varietà perfette, le varietà di Veronese, di Segre, di Grassmann (oltre alle varietà intersezioni complete).

appartengono a $\mathrm{syz}^1\mathfrak{a}$ e si ha precisamente (cfr. [98]): $\mathrm{syz}^1\mathfrak{a} = A\alpha_1 + A\alpha_2 + A\alpha_3 + A\alpha_4$.

D'altra parte, gli elementi $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ sono linearmente dipendenti su A, giacché:

$$X_3\alpha_1 - X_2\alpha_2 + X_1\alpha_3 - X_0\alpha_4 = 0;$$

si dimostra poi (cfr. [98]) che il modulo $\mathrm{syz}^2\mathfrak{a}$ è generato su A dalla quaterna $(X_3, -X_2, X_1, -X_0)$.

Ne segue, essendo $\mathrm{syz}^i\mathfrak{a} = 0$, per $i > 2$, che: $\mathrm{pd}\,\mathfrak{a} \geqslant 2$ (cfr. [12, (29.3)]), da cui (cfr. [31, p. 169, Th. 2]): $\mathrm{pd}\, A/\mathfrak{a} \geqslant 3$, mentre $\mathrm{gr}\,\mathfrak{a} = \mathrm{ht}\,\mathfrak{a} = 2$. Dunque $\mathfrak{a}$ non è un ideale perfetto.

Alcune proprietà delle risoluzioni libere finite

Vogliamo mostrare innanzitutto che l'esistenza di moduli che possiedono una FFR su un anello noetheriano locale A è intimamente connessa con l'esistenza di successioni regolari in A.[8]

Infatti, se M è un A-modulo di tipo finito non nullo tale che $\mathrm{pd}_A M = n$, nel qual caso M possiede certamente una FFR di lunghezza n,[9] allora A possiede una successione regolare di lunghezza n. Basta osservare che, in virtú di 3.18, si ha: $\mathrm{gr}\, A = \mathrm{pd}_A M + \mathrm{gr}\, M$, da cui (tenendo presente che tutti i termini che intervengono in tale formula sono non negativi) si ricava $\mathrm{pd}_A M \leqslant \mathrm{gr}\, A$, donde la conclusione.

Viceversa, se $x_1, \dots, x_n$ è una A-successione, allora $A/(x_1, \dots, x_n)$ possiede una FFR. Infatti, denotato con F_i l'A-modulo libero sopra $\binom{n}{i}$ generatori (con $i < n$), diciamo $e_{j_0, \dots, j_{i-1}}$ $(1 \leqslant j_0 < \quad < j_{i-1} \leqslant n)$, definiamo un omomorfismo $d_i \colon F_i \to F_{i-1}$ nel modo seguente:

$$d_i(e_{j_0, \dots, j_{i-1}}) = \sum_{l=0}^{i-1} (-1)^l x_{j_l} e_{j_0, \dots, \hat{j}_l, \dots, j_{i-1}},$$

dove il simbolo $\hat{}$ indica l'omissione. Ebbene si verifica senza difficoltà che:

$$0 \to F_n \to \quad \to F_i \to F_{i-1} \to \quad \to F_1 \to F_0 \to A/(x_1, \dots, x_n) \to 0$$

[8] Si noti in proposito che il Teorema di Auslander-Buchsbaum-Serre può anche enunciarsi dicendo che "un anello locale noetheriano A è regolare $\Leftrightarrow$ ogni A-modulo di tipo finito possiede una FFR".

[9] Nel caso locale, le nozioni di risoluzione proiettiva e di risoluzione libera coincidono.

è una FFR,[10] e si ha inoltre $\mathrm{pd}_A A/(x_1, \ldots, x_n) = n$: la disuguaglianza $\leqslant$ è ovvia, l'altra discende direttamente da 3.15.

Osservazione 4.4. Conviene notare esplicitamente che la risoluzione libera finita sopra costruita per l'A-modulo $A/(x_1, \ldots, x_n)$ è stata ottenuta proprio utilizzando il complesso di Koszul $K(x_1, \ldots, x_n, A)$ introdotto nella sezione precedente (cfr. anche [11]).

Passiamo ora a enunciare alcune proprietà notevoli delle FFR, studiate in [6]:

(a) Se A è un anello noetheriano con la proprietà che ogni A-modulo di tipo finito possiede una FFR, allora anche l'anello dei polinomi $A[X_1, \ldots, X_n]$, con $n \geqslant 1$, gode di tale proprietà;

(b) Se A è un dominio noetheriano tale che ogni A-modulo finitamente generato possiede una FFR, allora A è un UFD;

(c) Se M è un modulo (su un anello arbitrario) che possiede una FFR, diciamo:

$$0 \to F_n \to F_{n-1} \to \quad \to F_1 \to F_0 \to M \to 0,$$

allora, denotato con r_i il rango[11] di $F_i (0 \leqslant i \leqslant n)$ e indicata con $\chi(M)$ la caratteristica di Eulero di M:

$$\chi(M) = r_0 - r_1 + r_2 - \quad + (-1)^n r_n,^{12}$$

si ha: $\chi(M) \geqslant 0$.

Il Teorema di Hilbert-Burch

Una delle motivazioni piú profonde per lo studio delle FFR proviene dall'algebra lineare, giacché "risolvere un sistema di equazioni lineari" significa, in breve, "trovare una risoluzione libera".[13]

Infatti, consideriamo un sistema di m equazioni lineari omogenee in n incognite, sopra un anello A, che possiamo riguardare come un

[10] Si noti che tale FFR è stata ottenuta senza utilizzare l'ipotesi che A sia noetheriano o locale.

[11] Ossia il numero degli elementi di una sua base: tale numero è un invariante [1, Cap. 2, Esercizio 11].

[12] Si dimostra in [6] che $\chi(M)$ è indipendente dalla particolare FFR considerata, sicché è un invariante di M; inoltre $\chi(M)$ è invariante anche per localizzazione.

[13] Si veda: D. Buchsbaum, D. Eisenbud, *On a problem in linear algebra*, in [19].

omomorfismo di A-moduli liberi, diciamo $\varphi: A^n \to A^m$.[14] Ora, se A è un campo, diciamo $A = K$, e $\psi: K^n \to K^m$ è un omomorfismo di K-spazi vettoriali di rango r, risolvere il sistema (di m equazioni lineari omogenee in n incognite, sopra K) associato a ψ equivale a trovare il nucleo di ψ: in tal caso, com'è noto, lo spazio delle soluzioni è generato esattamente da $n - r$ soluzioni linearmente indipendenti, ciò che non è piú vero, in generale, passando ai moduli. Ne segue che, volendo studiare le soluzioni di un sistema, diciamo $\varphi: A^n \to A^m$, si è condotti necessariamente a studiare le relazioni di dipendenza lineare tra gli elementi di un sistema minimale di soluzioni che generano tutte le soluzioni.[15]

Dunque, risolvere il sistema φ "significa" trovare una risoluzione libera (possibilmente finita) di Coker φ:

$$\to F_i \to F_{i-1} \to \qquad \to F_1 = A^n \xrightarrow{\varphi} A^m = F_0 .$$

D'altra parte, il Teorema delle sizigie di Hilbert fornisce una prima risposta incoraggiante a tale problema[16] e suggerisce altresí lo studio delle relazioni che intercorrono tra le applicazioni lineari che compaiono in una FFR.

Ebbene, un primo risultato in proposito è il seguente:

Teorema 4.5. *Sia A un anello noetheriano e sia:*

$$0 \to F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} A$$

una successione esatta di A-moduli, essendo F_1 e F_2 moduli liberi di rango, rispettivamente, n e $n - 1$. Allora esiste un elemento x che non è un divisore dello zero in A ed è tale che φ_1 può essere fattorizzato nel modo seguente:

$$\begin{tikzcd} F_1 \arrow[r] \arrow[d, phantom, "\wr|||"] & A \\ \overset{n-1}{\wedge} F_1^* \arrow[r, "\overset{n-1}{\wedge} \varphi_2^*"'] & \overset{n-1}{\wedge} F_2^* \cong A. \arrow[u, "x"'] \end{tikzcd}$$ [17]

[14] Con la convenzione di scegliere come basi in A^n e in A^m le rispettive basi canoniche.

[15] Conviene segnalare un classico risultato di McCoy (cfr. [6, p. 147]), relativo all'esistenza delle soluzioni, secondo cui "un sistema di m equazioni lineari omogenee in n variabili sopra un anello A possiede autosoluzioni $\Leftrightarrow$ esiste un elemento non nullo di A che annulla tutti i determinanti dei minori di ordine n della matrice dei coefficienti".

[16] Vedi nota 13.

[17] Con la notazione $F_1{}^*$ si indica, come al solito, il *duale* di F_1, ossia il modulo $\mathrm{Hom}_A(F_1, A)$.

Il Teorema 4.5, insieme al suo inverso,[18] fornisce una condizione necessaria e sufficiente affinché un complesso della forma: $0 \to A^{n-1} \to A^n \to A$ sia esatto.[19] Esso va sotto il nome di Teorema di Hilbert-Burch, in quanto è stato provato da Hilbert, nel caso in cui A è l'anello dei polinomi in due variabili a coefficienti in un campo, e successivamente è stato dimostrato in tutta generalità da Burch in [149] (per una dimostrazione elementare, cfr. [6, p. 148, Es. 8]).

Una delle conseguenze piú importanti del Teorema di Hilbert-Burch è un teorema di struttura per ideali perfetti di altezza 2, in un anello noetheriano locale A: precisamente, faremo vedere che "gli ideali perfetti di altezza 2 in A sono determinantali".

Infatti, se $\mathfrak{a}$ è un ideale perfetto di altezza 2 in A, si ha una successione esatta della forma:

$$0 \to F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} A \to A/\mathfrak{a} \to 0\,,$$

essendo F_1 e F_2 A-moduli liberi, con F_1 diciamo di rango n, sicché F_2 ha rango $n - 1$: possiamo dunque applicare il Teorema 4.5.

Allora, scelta una base in F_1, l'applicazione $\overset{n-1}{\bigwedge}\varphi_2^*$ ha come coordinate (ossia, come immagini degli elementi della base) esattamente i determinanti dei minori di ordine $n - 1$ di φ_2, ossia della matrice associata; d'altra parte, l'immagine di tale applicazione è un ideale, diciamo, $\mathfrak{b}$ di A tale che $x\mathfrak{b} = \mathfrak{a}$, essendo x un elemento non divisore dello zero in A (Teorema 4.5), sicché x risulta necessariamente invertibile in A,[20] donde la conclusione.

Il Teorema di Hilbert-Burch è stato utilizzato come modello per molte ricerche sulle FFR. Inoltre, esso è stato utilizzato nello studio di varie questioni riguardanti, tra l'altro, la teoria delle deformazioni (delle curve dello spazio) [145], le intersezioni complete residue [134], la fattorialità,[21] la congettura di Zariski-Lipman per le ipersuperfici[22] e il cosiddetto "problema di sollevamento" di Grothendieck.[23]

[18] Il quale vale però con qualche ipotesi restrittiva sull'anello A (per es., A locale); si veda: D. Eisenbud, *Some directions of recent progress in commutative algebra*, in [104].

[19] Si ottiene cosí (nel caso locale) una specie di parametrizzazione per gli ideali di A di dimensione proiettiva 1.

[20] In virtú del Teorema dell'ideale principale di Krull.

[21] Cfr. il lavoro di Eisenbud citato nella nota 18.

[22] Cfr. nota precedente.

[23] Cfr. il lavoro di Buchsbaum e Eisenbud citato nella nota 13, nonché: Buchsbaum, Eisenbud, *Lifting modules and a theorem on finite free resolutions*, in *Ring Theory*, Academic Press, New York 1972, pp. 63-74.

Infine segnaliamo che il Teorema in questione è stato esteso largamente da Buchsbaum e Eisenbud in [145], con riferimento ad un'arbitraria FFR, pervenendo ad alcuni notevoli teoremi di struttura.[24]

Ulteriori risultati

Ritorniamo per un momento a considerare un sistema di m equazioni lineari omogenee in n incognite, sopra un campo K, di rango r, diciamo, e identifichiamo un siffatto sistema con un omomorfismo di spazi vettoriali (di rango r) $\varphi\colon K^n \to K^m$. Allora è facile stabilire quando un sistema di soluzioni assegnato genera l'intero spazio delle soluzioni: com'è noto, ciò accade, se e soltanto se, il sistema assegnato genera uno spazio vettoriale di dimensione $n - r$. Ora, ciò può esprimersi anche dicendo che, se $\psi\colon K^p \to K^n$ è un omomorfismo tale che $\varphi \circ \psi = 0$, allora l'applicazione composta $K^p \xrightarrow{\psi} K^n \xrightarrow{\varphi} K^m$ è esatta $\Leftrightarrow$ ψ ha rango $n - r$.

È chiaro allora che quest'ultima proprietà, trasferita nell'ambito dei sistemi di equazioni a coefficienti in un anello, ha come analogo un criterio di esattezza per un complesso di moduli liberi:

$$\to F_n \to F_{n-1} \to \qquad \to F_1 \to F_0$$

almeno nel caso in cui esso è finito (ossia, $F_i = 0$, per $i \gg 0$).

Ebbene, un tale criterio di esattezza (stabilito peraltro in un contesto piú generale) è stato dato da Buchsbaum e Eisenbud in [144]. In particolare, esso fornisce una condizione necessaria e sufficiente affinché un complesso del tipo:

$$K\colon \qquad 0 \to F_n \to F_{n-1} \to \qquad \to F_1 \to F_0 \to 0\,,$$

dove gli F_i sono moduli liberi di tipo finito sopra un anello noetheriano è *aciclico*, ossia è esatto, fatta eccezione eventualmente in F_0, sicché K risulta una risoluzione libera finita di Coker $(F_1 \to F_0)$.

Conviene segnalare inoltre che da tale risultato si ottiene in particolare un corollario il quale estende (cfr. [29]) la cosiddetta "sensibilità rispetto alla profondità" del complesso di Koszul [136]:

[24] Da uno di essi si deduce, in particolare, un importante risultato di Mac Rae [204], secondo cui "se $\mathfrak{a}$ è un ideale generato da due elementi in un anello noetheriano arbitrario, allora si verifica necessariamente una delle seguenti eventualità: pd $\mathfrak{a} = 0$, pd $\mathfrak{a} = 1$, oppure pd $\mathfrak{a} = \infty$".

Proposizione 4.6. *Sia A un anello noetheriano, $\mathfrak{a} = (x_1, \ldots, x_n)$ un ideale arbitrario di A e M un A-modulo di tipo finito tale che $\mathfrak{a}M \neq M$. Sia K il complesso di Koszul $K(x_1, \ldots, x_n, M)$*[25] *e sia d il piú grande intero tale che $H_d(K) \neq 0$.*[26]

Allora $\mathrm{gr}_A(\mathfrak{a}, M)$, ossia il grado di $\mathfrak{a}$ su M, è uguale al numero dei moduli di omologia del complesso di Koszul che si annullano consecutivamente, contando dalla sinistra.

Recentemente, Buchsbaum e Eisenbud hanno dimostrato in [147] alcuni notevoli teoremi di struttura per ideali di altezza 3, tra cui, in particolare, uno relativo agli ideali di Gorenstein di altezza 3,[27] analogo[28] al teorema di struttura di Hilbert per gli ideali perfetti di altezza 2.

Osservazione 4.7. Conviene sottolineare che l'interesse per gli ideali di Gorenstein di altezza 3 è dovuto al fatto che, se l'altezza è < 3, il comportamento di siffatti ideali è noto ed è alquanto semplice. Infatti, nel 1960, Serre ha dimostrato [235] che "se $\mathfrak{a}$ è un ideale di Gorenstein di altezza 2 in un anello locale regolare, allora $\mathfrak{a}$ può essere generato da due elementi (ossia, $\mathfrak{a}$ è un'intersezione completa)".[29] Ebbene, ciò non è piú vero per ideali di Gorenstein di altezza 3. L'esempio classico è il seguente: Sia k un campo e sia $A = k[[X, Y, Z]]/(X^2 - Y^2, Y^2 - Z^2, XY, YZ, ZX)$, sicché A è locale, con ideale massimale $\mathfrak{m} = (x, y, z)$. Allora si verifica facilmente che $\mathrm{Ann}(\mathfrak{m}) = (x^2)$, il quale è uno spazio vettoriale di dimensione 1 su $A/\mathfrak{m}$, e quindi [6, Th. 221] A è di Gorenstein, ma d'altra parte l'ideale $(X^2 - Y^2, Y^2 - Z^2, XY, YZ, ZX)$ in $k[[X, Y, Z]]$ chiaramente non può essere generato da tre elementi, ossia, A non è un'"intersezione completa".

Aggiungiamo inoltre che in [147], come conseguenza del teorema di struttura, si dimostra che il numero minimo di generatori di un

[25] Denotiamo con tale simbolo il complesso $K(x_1, \ldots, x_n, A) \otimes_A M$ (cfr. anche [11]).

[26] Si noti che $H_0(K) \cong M/\mathfrak{a}M$, sicché risulta: $0 < d \leq n$.

[27] Un ideale $\mathfrak{a}$ di un anello locale regolare A si dice di Gorenstein, se $A/\mathfrak{a}$ è un anello di Gorenstein.

[28] Nel senso che esso fornisce la "forma generica" per un ideale di Gorenstein di altezza 3, la quale risulta però piú complicata, rispetto, per es., a quella data dal Teorema di Hilbert-Burch, in quanto in essa compaiono oltre ai determinanti anche i pfaffiani di certe matrici (per la definizione di pfaffiano, cfr. [16]).

[29] È chiaro, in virtú di 3.32, che ogni ideale di Gorenstein di altezza 1 in un anello locale regolare è principale.

ideale di Gorenstein di altezza 3 è necessariamente dispari (cfr. anche [49]),[30] e vengono date altresí delle applicazioni a talune questioni collegate alla "liaison" di varietà algebriche (cfr. [134] e [218]).

Segnaliamo infine la soluzione, data da A. Lascoux [198], al problema di studiare la catena delle sizigie di un ideale di minori di un certo ordine della *matrice generica* $m \times n$ sopra un anello commutativo.

Alcuni problemi aperti

Ci limitiamo in questo paragrafo ad accennare brevemente a taluni, tra i piú significativi e ricchi di conseguenze, dei numerosi problemi aperti nell'ambito della teoria omologica dei moduli, rinviando, per un'esposizione pressoché completa, direttamente alla monografia di Hochster [29] e alla memoria di Peskine e Szpiro [217].

1) *Il problema della "molteplicità di intersezione"*[31]

Sia A un anello locale regolare, $\mathfrak{m}$ il suo ideale massimale, e siano M, N due A-moduli di tipo finito tali che $M \otimes_A N$ abbia lunghezza finita, brevemente: $l(M \otimes_A N) < \infty$.[32] In tal caso, per ogni $i \geqslant 0$, $\mathrm{Tor}_i^A(M, N)$ ha lunghezza finita,[33] e quindi ha senso definire la *molteplicità di intersezione* $e_A(M, N)$ nel modo seguente:

$$e_A(M, N) = \sum_{i \geqslant 0} (-1)^i \, l(\mathrm{Tor}_i^A(M, N)).^{34}$$

Ora la molteplicità di intersezione cosí definita gode di alcune notevoli proprietà [52]:

[30] Tale risultato era stato ottenuto indipendentemente da Watanabe, nel 1973. Si noti inoltre che in [147] vengono dati degli esempi di ideali di Gorenstein di altezza 3 in $k[[X, Y, Z]]$, con k campo, tali che il minimo numero di generatori è un arbitrario intero dispari $n \geqslant 3$ (prefissato).

[31] Una trattazione omologica della molteplicità di intersezione si trova sviluppata in [52].

[32] Ciò equivale al fatto che l'ideale $\mathrm{Ann}(M) + \mathrm{Ann}(N)$ è $\mathfrak{m}$-primario: infatti [11, p. 72], se M è un modulo non nullo finitamente generato su un anello noetheriano, si ha: $l(M) < \infty \Leftrightarrow \dim M = \dim A/\mathrm{Ann}(M) = 0$, da cui la tesi, tenendo presente [1, Cap. 3, Es. 19] che $V(\mathrm{Ann}(M \otimes_A N)) = V(\mathrm{Ann}(M) + \mathrm{Ann}(N))$.

[33] Infatti, nelle ipotesi attuali, $\mathrm{Tor}_i^A(M, N)$ è annullato da $\mathrm{Ann}(M) + \mathrm{Ann}(N)$ per ogni i.

[34] Si noti (cfr. ad es. [52, IV-34, Th. 8]) che non è restrittivo supporre $i \leqslant \dim A$, nella sommatoria.

Teorema 4.8. *Sia A un anello locale regolare contenente un campo (o più in generale, tale che il suo completamento $\hat{A}$ sia un anello di serie di potenze formali sopra un anello di valutazione discreta completo), e siano M, N due A-moduli di tipo finito tali che $l(M \otimes_A N) < \infty$. Allora si ha:*

i) $e_A(M, N) \geqslant 0$;

ii) $\dim M + \dim N \leqslant \dim A$;

iii) $\dim M + \dim N < \dim A \Leftrightarrow e_A(M, N) = 0$.

Ebbene Serre congetturò in [52] che tale risultato continuasse a valere per un anello locale regolare qualsiasi (ciò è stato dimostrato vero, per ogni anello locale regolare di dimensione $\leqslant 4$, da Hochster [19, pp. 120-152]).[35]

Piú in generale (e piú ottimisticamente[36]) Peskine e Szpiro hanno congetturato [217] che il Teorema 4.8 continui a valere per un anello locale noetheriano qualsiasi A e per due A-moduli M, N di tipo finito tali che $l(M \otimes_A N) < \infty$ e inoltre $\mathrm{pd}_A M < \infty$ (nel qual caso è possibile dare la stessa definizione formale per la molteplicità di intersezione $e_A(M, N)$).

Osservazione 4.9. Conviene notare esplicitamente che il caso piú importante della molteplicità di intersezione è quello che corrisponde alla situazione geometrica, e dunque, in prima istanza, il caso in cui $M = A/\mathfrak{p}$ e $N = A/\mathfrak{q}$, con $\mathfrak{p}$, $\mathfrak{q}$ ideali primi di un anello locale regolare "geometrico" A. Analizziamo in proposito un esempio elementare:

Sia A l'anello locale del piano affine $\mathbf{A}_k^2$ (con k campo algebricamente chiuso) nell'origine, dunque $A = k[X, Y]_{(X,Y)}$, e siano C e D due curve piane passanti per l'origine (irriducibili o piú in generale) prive di componenti comuni passanti per l'origine, definite rispettivamente da polinomi F e G. Denotiamo poi, rispettivamente con x, y, f e g, le immagini, in A, di X, Y, F e G. Ora, posto: $M = A/(f)$ e $N = A/(g)$, è subito visto che il modulo $M \otimes_A N$ ha lunghezza finita (giacché, in virtú delle ipotesi fatte su C e D, l'ideale (f, g) è certamente (x, y)-primario). Allora, la molteplicità di intersezione è data da:

$$e_A(M, N) = l(\mathrm{Tor}_0^A(M, N)) - l(\mathrm{Tor}_1^A(M, N)) + l(\mathrm{Tor}_2^A(M, N)).$$

[35] Cfr. anche [145] per alcune applicazioni a tale congettura dei teoremi di struttura relativi alle risoluzioni libere finite.

[36] Sulla base di alcuni risultati incoraggianti da essi ottenuti, nel caso graduato.

A questo punto, osserviamo che:

(a) $\mathrm{Tor}_2^A(M, N) = 0$: infatti, si ha (3.19): $\mathrm{gr}\, M \leqslant \dim M = \dim A/(f) = 1$, da cui chiaramente $\mathrm{gr}\, M = 1$; ma allora (3.18, 3.30) $\mathrm{pd}_A M = 1$, donde la tesi, in virtú di [52, IV-34, Th. 8];

(b) $\mathrm{Tor}_1^A(M, N) = 0$: infatti, nelle ipotesi attuali (cfr. [59, p. 126, Ex. 19]) si ha: $\mathrm{Tor}_1^A(M, N) = \mathrm{Tor}_1^A(A/(f), A/(g)) \cong (f) \cap (g)/(fg)$ da cui la tesi, in virtú di 3.32.

Dunque la molteplicità di intersezione è data, nel nostro caso, da $l(\mathrm{Tor}_0^A(M, N)) = l(A/(f, g)) = \dim_k(A/(f, g))$, essendo k il campo residuo di A: si riottiene cosí la nozione "classica" di molteplicità di intersezione (cfr. ad es. [94], [103]).

2) *Il problema della "rigidità" dei* Tor

Nel 1966, Lichtenbaum riuscí a dimostrare ("Ill. J. Math.", *10*, 1966, pp. 220-226), estendendo un risultato di M. Auslander, che "se A è un anello locale regolare e M, N sono A-moduli finitamente generati e tali che $\mathrm{Tor}_i^A(M, N) = 0$, per qualche $i \geqslant 0$, allora $\mathrm{Tor}_j^A(M, N) = 0$, per ogni $j > i$".

Ebbene sorge spontaneo il problema di chiedersi se una tale proprietà, detta anche *proprietà di rigidità* per M, continua a valere per un anello noetheriano qualsiasi, purché $\mathrm{pd}\, M < \infty$. Precisamente:

Congettura (A). Sia A un anello noetheriano e siano M, N due A-moduli di tipo finito, e supponiamo che $\mathrm{pd}_A M < \infty$. Allora, se $\mathrm{Tor}_i^A(M, N) = 0$, per un certo indice $i\ (> 0)$, risulta: $\mathrm{Tor}_j^A(M, N) = 0$, per ogni $j > i$.[37]

Tale congettura (certamente vera, se $\mathrm{pd}_A M = 1$) è stata provata in [217] nel caso in cui $\mathrm{pd}_A M = 2$ e inoltre $\mathrm{Ann}(M) \neq 0$. Essa è vera anche se $M = A/(x_1, \ldots, x_n)$, dove $x_1, \ldots, x_n$ è una A-successione.

Inoltre, la congettura (A) ha come conseguenza una classica congettura di Auslander:

Congettura (B). Sia A un anello locale noetheriano, M un A-modulo di tipo finito e di dimensione proiettiva finita, e x un elemen-

[37] Si noti che il problema analogo, enunciato con riferimento agli indici $j < i$, ammette in generale risposta negativa.

to di A. Allora, se x non è un divisore dello zero per M, x non è un divisore dello zero in A.[38]

3) *Il problema della "proprietà dell'intersezione" per un anello locale*

Tale problema può essere enunciato nella forma seguente:

Congettura (C). Sia A un anello noetheriano locale e siano M, N A-moduli di tipo finito, con $M \neq 0$, tali che $M \otimes_A N$ abbia lunghezza finita. Allora si ha: $\dim N \leqslant \mathrm{pd}_A M$.

Tale congettura è stata provata per anelli locali di caratteristica $p > 0$, da Peskine e Szpiro, i quali hanno dimostrato altresí che (A) $\Rightarrow$ (C) $\Rightarrow$ (B) per ogni classe di anelli locali chiusi rispetto alle operazioni seguenti: il completamento, la localizzazione rispetto a un ideale primo e il passaggio ad un'immagine omomorfa.

Osserviamo inoltre che la congettura (C) è equivalente [19, pp. 120-152] ad un'estensione "omologica" del Teorema dell'ideale principale di Krull. Per di piú, com'è stato dimostrato da Peskine e Szpiro, essa implica (per una vasta classe di anelli) la cosiddetta "congettura di Bass":

Congettura (D). Sia A un anello locale noetheriano che possiede un modulo T non nullo di tipo finito e di dimensione iniettiva finita. Allora A è un anello di Cohen-Macaulay.

Per finire, segnaliamo una notevole congettura di Hochster:

Congettura (E). Sia A un anello locale noetheriano e sia $x_1, \ldots, x_n$ un sistema di parametri. Allora esiste un A-modulo M (non necessariamente di tipo finito) tale che $x_1, \ldots, x_n$ è una M-successione.[39]

Essa è chiamata la "Big Cohen-Macaulay modules conjecture", poiché un modulo M siffatto risulta certamente di Cohen-Macaulay, se è finitamente generato. Infatti, in tal caso si ha (3.19): $\mathrm{gr}\, M \leqslant \dim M \leqslant \dim A = n$, e d'altra parte $n \leqslant \mathrm{gr}\, M$ (3.12), donde la conclusione. Lo studio di tale congettura ha gettato nuova luce su numerose altre congetture nella teoria omologica degli anelli commutativi, chiarificando altresí i mutui rapporti tra di esse (cfr. [29]).

[38] Tale congettura è stata dimostrata da Peskine e Szpiro in [217] nel caso in cui A contiene un campo di caratteristica $p > 0$, oppure è una k-algebra "essenzialmente di tipo finito" (per la def., cfr. [101, (0; (6.3.14))]), essendo k un campo.

[39] Essa è stata provata da Hochster [29] nel caso in cui A (o piú in generale $A/\mathfrak{N}$, essendo $\mathfrak{N}$ il nilradicale di A) contiene un campo.

5.

Alcuni risultati e problemi relativi alle varietà intersezioni complete

Introduzione

Il problema delle intersezioni complete in geometria algebrica consiste, in breve, nello studio delle varietà algebriche di uno spazio affine o proiettivo, le quali possono venir definite come intersezioni di un numero "giusto" di ipersuperfici (dello spazio ambiente). È chiaro allora che tale problema, tradotto in termini algebrici, diventa un problema relativo al numero "giusto" (e in particolare, al numero minimo) di elementi che generano un ideale di un anello di polinomi: ciò giustifica le considerazioni appresso sviluppate.

Sia $\mathfrak{a}$ un ideale di un anello noetheriano A e denotiamo con $\mu(\mathfrak{a})$ il numero minimo di generatori di $\mathfrak{a}$. Ne segue [1, Cor. 11.16], che $\mu(\mathfrak{a}) \geqslant \operatorname{ht} \mathfrak{a}$.[1]

Def. 5.1. Un ideale $\mathfrak{a}$ di un anello noetheriano A si dice un ideale *intersezione completa* (*in senso stretto*), se soddisfa alla condizione: $\mu(\mathfrak{a}) = \operatorname{ht} \mathfrak{a}$.

Def. 5.2. Un ideale $\mathfrak{a}$ di un anello noetheriano A si dice un ideale *localmente intersezione completa*, se, per ogni ideale massimale $\mathfrak{m}$ di A, si ha: $\mu(\mathfrak{a}_\mathfrak{m}) = \operatorname{ht} \mathfrak{a}_\mathfrak{m}$.

Def. 5.3. Un ideale $\mathfrak{a}$ di un anello noetheriano A si dice un ideale *intersezione completa in senso insiemistico*, se, posto $\operatorname{ht} \mathfrak{a} = t$, esistono t elementi in A, diciamo $f_1, \ldots, f_t$ tali che: $r(\mathfrak{a}) = r((f_1, \quad, f_t))$.[2]

[1] Supporremo sempre tacitamente che gli ideali in esame abbiano altezza $\geqslant 1$.

[2] È chiaro che un ideale intersezione completa (in senso stretto) è anche intersezione completa in senso insiemistico.

Osserviamo innanzitutto che le nozioni ora introdotte hanno un chiaro significato geometrico. Infatti, se ad esempio, V è una varietà algebrica[3] di dimensione d di uno spazio affine $\mathbf{A}_k^n$ (essendo k un campo algebricamente chiuso arbitrario) e $\mathfrak{a} = \mathcal{I}(V)$ è l'ideale di $k[X_1, \ldots, X_n]$ associato a V,[4] allora in corrispondenza alle definizioni sopra introdotte, si ha, rispettivamente:

(1) V è un'intersezione completa (in senso stretto) di $n - d$ ipersuperfici (di $\mathbf{A}^n$);

(2) V è localmente, ossia in ogni punto, intersezione del numero "giusto" di ipersuperfici;

(3) V può essere definita come l'insieme dei punti comuni a $n - d$ ipersuperfici, precisamente: $V = \bigcap_{i=1}^{t} V(f_i)$.

Osservazione 5.4. Si noti, con riferimento alla Def. 5.1, che, se A è un anello di Cohen-Macaulay (per es. $A = k[X_1, \ldots, X_n]$, con k campo), le seguenti condizioni sono equivalenti per un ideale $\mathfrak{a}$ di A:

i) $\mu(\mathfrak{a}) = \mathrm{ht}\, \mathfrak{a}$;

ii) $\mu(\mathfrak{a}) = \mathrm{gr}\, \mathfrak{a}$;

iii) $\mathfrak{a}$ è generato da una A-successione.[5]

Infatti, si ha in generale (3.10 (d)): $\mathrm{gr}\, \mathfrak{a} \leqslant \mathrm{ht}\, \mathfrak{a} \leqslant \mu(\mathfrak{a})$, da cui: (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i); inoltre, sempre per un anello noetheriano qualsiasi, si ha (3.14): (ii) $\Rightarrow$ (iii). Infine, essendo A un anello CM, si ha, in virtú di 3.23, che (i) $\Rightarrow$ (ii) donde la conclusione.

Esempi 5.5. (1) Consideriamo la cubica sghemba C di $\mathbf{A}_k^3$ (essendo k un campo algebricamente chiuso, come al solito) di equazioni parametriche: $X = t$, $Y = t^2$, $Z = t^3$ ($t \in k$). Ebbene C è un'intersezione completa di due superfici di $\mathbf{A}^3$.[6]

Infatti, cominciamo coll'osservare che lo spazio vettoriale (su k) delle quadriche di $\mathbf{A}^3$ passanti per C è generato dalle quadriche, dicia-

[3] Per "varietà" intenderemo sempre (salvo ulteriori specificazioni) un insieme algebrico *puro*, ossia tale che tutte le sue componenti irriducibili [103] abbiano la medesima dimensione.

[4] Cfr. [1, Cap. 1, Esercizio 27] e, per ulteriori proprietà [103].

[5] È chiaro che l'equivalenza di tali condizioni, per ogni ideale di A, caratterizza gli anelli di Cohen-Macaulay. Segnaliamo inoltre alcuni risultati generali relativi al numero minimo di generatori di un ideale massimale in un anello di polinomi, ottenuti da E. D. Davis e A. V. Geramita ("Trans. Amer. Math. Soc.", *231*, 1977, pp. 497-505).

[6] È subito visto che C è una curva irriducibile non singolare.

mo F_1, F_2, F_3, di equazioni, rispettivamente:

$$XZ - Y^2 = 0\,, \quad X^2 - Y = 0\,, \quad XY - Z = 0\text{[7]};$$

si verifica subito che C è l'insieme dei punti comuni alle quadriche F_2 e F_3. Piú precisamente, considerando l'omomorfismo di k-algebre $\varphi\colon k[X, Y, Z] \to k[t]$, definito ponendo: $\varphi(X) = t$, $\varphi(Y) = t^2$, $\varphi(Z) = t^3$, si conclude che $\operatorname{Ker}\varphi = (X^2 - Y, XY - Z)(= \mathscr{I}(C))$, sicché C risulta l'intersezione completa (in senso stretto) di F_2 e F_3.

Ciò non è piú vero, se si considera la cubica sghemba proiettiva $\bar{C}$[8] di $\mathbf{P}^3$. Infatti, in tal caso (cfr. [111, pp. 20-21]) si ha: $\mathscr{I}(\bar{C}) = (XZ - Y^2, X^2 - YW, XY - ZW)$[9]; ora, se per assurdo esistessero due polinomi (omogenei) f e g in $k[X, Y, Z, W]$ tali che $\mathscr{I}(\bar{C}) = (f, g)$, si avrebbe senz'altro che f e g sono polinomi di secondo grado,[10] dunque f e g andrebbero scelti fra i tre generatori sopra scritti per $\mathscr{I}(\bar{C})$, ciò che è una contraddizione.[11] Segnaliamo tuttavia che $\bar{C}$ è un'intersezione completa in senso insiemistico di due superfici, per es. della quadrica $\bar{F}_2$[12] di equazione: $X^2 - YW = 0$ e della superficie cubica G di equazione: $Y^3 - 2XYZ + Z^2W = 0$. Infatti, basta osservare che, se $P = (X, Y, Z, 1)$ è un punto "al finito" appartenente a $\bar{F}_2 \cap G$, si ha: $Y = X^2$ e $(X^3 - Z)^2 = 0$, ossia $P \in \bar{C}$ e inoltre l'unico punto "all'infinito" di $\bar{F}_2 \cap G$ è esattamente il punto $(0, 0, 1, 0)$, ossia il punto "all'infinito" di $\bar{C}$: dunque $\bar{F}_2 \cap G \subseteq \bar{C}$; d'altra parte, l'inclusione in senso opposto è immediata, poiché si ha: $Y^3 - 2XYZ + Z^2W = -Y(XZ - Y^2) - Z(XY - ZW)$.[13]

(2) Consideriamo la quintica sghemba $\mathscr{D}$ di $\mathbf{A}^3_k$ di equazioni parametriche: $X = t^3, Y = t^4, Z = t^5$; si verifica facilmente che si tratta di una curva irriducibile avente un unico punto singolare nell'origine $(0, 0, 0)$. È chiaro che $\bar{\mathscr{D}}$[14] non è un'intersezione completa: basta os-

[7] Le quali risultano senz'altro linearmente indipendenti su k; si ha inoltre: $XZ - Y^2 = Y(X^2 - Y) - X(XY - Z)$.

[8] Se V è una varietà di uno spazio affine $\mathbf{A}^n$, denotiamo con $\bar{V}$ la chiusura proiettiva di V in $\mathbf{P}^n$ (cfr. [94] oppure [103]).

[9] Essendo $\mathscr{I}(\bar{C})$ l'ideale omogeneo associato a $\bar{C}$ in $k[X, Y, Z, W]$.

[10] Le altre eventualità si scartano subito con calcoli diretti.

[11] Basta osservare che le tre quadriche (corrispondenti ai generatori di $\mathscr{I}(\bar{C})$) si intersecano a due a due in $\bar{C}$ e in rette a due a due distinte. Diversamente, si può concludere utilizzando il Teorema di Bézout [120].

[12] Vedi nota 8.

[13] Piú precisamente, la curva in questione risulta un'intersezione completa insiemistica, con molteplicità 2.

[14] Vedi nota 8.

servare, ad es., che il suo ordine è un numero primo e utilizzare il Teorema di Bézout [120]; si dimostra poi[15] che anche $\mathscr{D}$ non è (neppure localmente) un'intersezione completa. Tuttavia, con un'argomentazione analoga a quella sopra sviluppata, si prova che $\mathscr{D}$ risulta un'intersezione completa insiemistica[16] della superficie cubica di eq. $Z^2 - X^2Y = 0$ e della superficie quartica di eq. $X^4 + Y^3 - 2XYZ = 0$.

(3) Consideriamo, per ogni intero $d \geqslant 4$, la curva C_d di $\mathbf{P}_k^3$ di equazioni parametriche: $X = tu^{d-1}$, $Y = t^{d-1}u$, $Z = t^d$, $W = u^d$: è subito visto che si tratta di una curva irriducibile non singolare di ordine d. Si dimostra (cfr. [180]) che, se k è un campo algebricamente chiuso di caratteristica $p > 0$, allora C_d risulta un'intersezione completa in senso insiemistico, per ogni $d \geqslant 4$; invece, se k ha caratteristica zero, non si sa (neppure per $d = 4$) se tali curve sono intersezioni complete in senso insiemistico (cfr. anche [102, p. 125]).

Il caso "forte"

Cominciamo col dimostrare un risultato, stabilito essenzialmente in [235], il quale mette in evidenza i legami alquanto profondi (e storicamente molto importanti) tra il problema delle intersezioni complete (in senso stretto) e la Congettura di Serre sui moduli proiettivi.

Teorema 5.6. *Sia* $\mathfrak{a}$ *un ideale di altezza* 2 *nell'anello* $A = k[X_1, \ldots, X_n]$, *essendo* k *un campo arbitrario. Allora le seguenti condizioni sono tra loro equivalenti:*

(1) $\mathfrak{a}$ *è un ideale intersezione completa*;

(2) $\mathfrak{a}$ *soddisfa alle seguenti condizioni*:

i) $\operatorname{pd} \mathfrak{a} \leqslant 1$,

ii) $\operatorname{Ext}_A^1(\mathfrak{a}, A)$ *è un* A*-modulo ciclico.*

Dimostrazione. (1) $\Rightarrow$ (2). La (i) si ottiene subito osservando che, posto $\mathfrak{a} = (f, g)$, ciò che è lecito nelle ipotesi attuali, $\mathfrak{a}$ possiede una risoluzione libera data da:

$$\text{(I)} \qquad 0 \to A \xrightarrow{\psi} A^2 \xrightarrow{\varphi} \mathfrak{a} \to 0,$$

[15] Cfr. [178].
[16] Vedi nota 13.

dove φ e ψ sono definiti, rispettivamente, ponendo: $\varphi(1, 0) = f$, $\varphi(0, 1) = g$ e $\psi(1) = (-g, f)$, (cfr. 3.7).

Inoltre, scrivendo la successione esatta degli Ext, $\mathrm{Ext}(-, A)$, ottenuta a partire dalla (I), si ha (Sez. 3, nota 7):

$$\to A \cong \mathrm{Hom}_A (A, A) \to \mathrm{Ext}^1_A (\mathfrak{a}, A) \to \mathrm{Ext}^1_A (A^2, A) \to$$

da cui, avendosi $\mathrm{Ext}^1_A (A^2, A) = 0$ (essendo A^2 proiettivo su A[17]), si deduce che $\mathrm{Ext}^1_A (\mathfrak{a}, A)$ è un'immagine epimorfa di A, ossia (ii).

$(2) \Rightarrow (1)$. Infatti, sia ξ un generatore di $\mathrm{Ext}^1_A (\mathfrak{a}, A)$[18] e consideriamo un rappresentante della classe di estensioni data da ξ:

$$\text{(II)} \qquad 0 \to A \to E \to \mathfrak{a} \to 0.$$

Allora, dalla successione esatta degli Ext, $\mathrm{Ext}(-, A)$, si ha:

$$\begin{aligned} &\to \mathrm{Hom}_A (A, A) \xrightarrow{\varphi} \mathrm{Ext}^1_A (\mathfrak{a}, A) \to \\ &\to \mathrm{Ext}^1_A (E, A) \to \mathrm{Ext}^1_A (A, A) = 0, \end{aligned}$$

da cui si ricava subito che $\mathrm{Ext}^1_A (E, A) = 0$, giacché l'omomorfismo di connessione φ porta l'elemento unità di A nel generatore ξ di $\mathrm{Ext}^1_A (\mathfrak{a}, A)$, (cfr. [65] o [66]), dunque è suriettivo.

[17] Cfr. la nota 8 della sezione 3 oppure la nota che segue.

[18] Ricordiamo (cfr. [65] o [66]) che $\mathrm{Ext}^1_A (M, N)$ può essere introdotto anche come un modello dell'insieme delle soluzioni del cosiddetto "problema di estensione" che consiste nello studio di tutte le successioni esatte essenzialmente distinte, della forma: $0 \to N \to E \to M \to 0$, che prendono il nome di "estensioni di N mediante M". Ora, nell'insieme di siffatte estensioni si introduce una relazione di equivalenza, chiamando *equivalenti* due estensioni $0 \to N \to E \to M \to 0$ e $0 \to N \to E' \to M \to 0$, se esiste un omomorfismo $h : E \to E'$ tale che il diagramma seguente:

$$\begin{tikzcd} 0 \arrow[r] & N \arrow[r] \arrow[d, "j"] & E \arrow[r] \arrow[d, "h"] & M \arrow[r] \arrow[d, "i"] & 0 \\ 0 \arrow[r] & N \arrow[r] & E' \arrow[r] & M \arrow[r] & 0 \end{tikzcd}$$

(essendo i e j omomorfismi identità) è commutativo, nel qual caso h risulta un isomorfismo. Ebbene si dimostra che l'insieme delle classi di equivalenza di tali estensioni possiede una struttura di A-modulo e risulta inoltre isomorfo al modulo $\mathrm{Ext}^1_A (M, N)$ definito in precedenza (Sezione 3, nota 7). Si ottiene in particolare [65, Ch. 3] che:

(a) $\mathrm{Ext}^1_A (M, N) = 0 \Leftrightarrow$ ogni estensione di N mediante M è *spezzata*, ossia $E \cong M \oplus N$ (ciò che accade, ad es., se M è proiettivo);

(b) $\mathrm{Ext}^1_A (M, N_1 \oplus N_2) \cong \mathrm{Ext}^1_A (M, N_1) \oplus \mathrm{Ext}^1_A (M, N_2)$, essendo N_1, N_2 A-moduli arbitrari.

D'altra parte, stante la (II), si ha: pd $E \leqslant 1$[19]; allora, se consideriamo una risoluzione proiettiva di lunghezza 1 di E, diciamo $0 \to P \to Q \to E \to 0$, e supponiamo che $P \cong A^r$, essendo r un intero positivo opportuno,[20] otteniamo:

$$\mathrm{Ext}^1_A(E, P) \cong \bigoplus^r \mathrm{Ext}^1_A(E, A) = 0.$$

Ne segue in particolare che $Q = P \oplus E$, dunque E è un A-modulo proiettivo di rango 2[21]; ma allora E risulta un A-modulo libero di rango 2,[22] ossia $E \cong A^2$ e pertanto, stante la (II), $\mathfrak{a}$ può essere generato da due polinomi, donde la conclusione.

Osservazione 5.7. (a) Si noti, con riferimento all'enunciato del Teorema 5.6, che la condizione (i) può essere sostituita dalla condizione seguente (j) "$\mathfrak{a}$ è puro ed è localmente intersezione completa".

Infatti, segue subito da (1) che $\mathfrak{a}$ è puro (giacché A è CM) e localmente intersezione completa (basta localizzare). D'altra parte (j) $\Rightarrow$ (i), poiché, nelle ipotesi attuali, la condizione pd $\mathfrak{a} \leqslant 1$ è locale (3.4).

(b) È chiaro che, alla luce della soluzione del Problema di Serre sui moduli proiettivi, la condizione (2) (i) del Teorema 5.6 può essere riscritta nella forma: pd $\mathfrak{a} = 1$.

Corollario 5.8. *Sia C una curva irriducibile non singolare di $\mathbf{A}^3_k$, essendo k un campo algebricamente chiuso, e sia $\mathfrak{a} = \mathscr{I}(C)$ l'ideale associato a C nell'anello $A = k[X, Y, Z]$. Allora C è un'intersezione completa $\Leftrightarrow$ il modulo dei differenziali $\Omega_k(A/\mathfrak{a})$[23] è ciclico, come $A/\mathfrak{a}$-modulo.*[24]

Dimostrazione. Infatti, basta tener presente che, nelle ipotesi attuali, si ha (cfr. [235] oppure [216]): $\mathrm{Ext}^1_A(\mathfrak{a}, A) \cong \Omega^1_k(A/\mathfrak{a})$ e inoltre che l'ideale $\mathfrak{a} = \mathscr{I}(C)$ soddisfa certamente alla condizione (j) enunciata nell'Oss. 5.7 (a).

[19] Si ha infatti, in virtù di un risultato generale (cfr. ad es. [6, p. 124, Th. B]): pd $E \leqslant \max$ (pd A, pd $\mathfrak{a}$).

[20] Ciò non è restrittivo: basta sommare (eventualmente) un modulo proiettivo di tipo finito con P e Q.

[21] Ciò segue dalla (II), ricordando che, se M è un modulo di tipo finito su un dominio di integrità A, con campo dei quozienti K, si definisce *rango* di M e si denota con rg M, la dimensione del K-spazio vettoriale $M \otimes_A K$.

[22] Ecco il punto cruciale in cui interviene la validità della Congettura di Serre (limitatamente ai moduli proiettivi di tipo finito di rango 2 su A).

[23] Per la definizione e le prime proprietà di tale modulo, cfr. [11].

[24] Un risultato analogo relativo alle varietà irriducibili non singolari di codimensione 2 di $\mathbf{A}^n$ si trova in [235].

Corollario 5.9. *Ogni curva irriducibile non singolare di genere* $\leqslant 1$ *di* $\mathbf{A}^3_k$ *è un'intersezione completa.*

Dimostrazione. Infatti ogni curva siffatta verifica (cfr. ad es. [121]) la condizione sul modulo dei differenziali enunciata in 5.8.[25]

Osservazione 5.10. (a) Si noti che la caratterizzazione data in 5.8 per le curve di $\mathbf{A}^3$ che sono intersezioni complete, dipende soltanto dall'anello delle coordinate. Un risultato ancora piú "intrinseco", indipendente dall'immersione delle curve in questione (e valido piú in generale per le varietà di codimensione 2 di $\mathbf{A}^n$) è stato ottenuto recentemente da N. Mohan Kumar (*Complete intersections*, in "J. Math. Kyoto Univ.", *17*, 1977, pp. 533-538).

(b) Il Corollario 5.9 non continua a valere per una curva irriducibile non singolare di genere > 1 (un controesempio esplicito relativo ad una curva siffatta di genere 2 si trova in [207]), e neppure per curve singolari (cfr. 5.5 (2) e la nota 10 della sezione 2).

(c) Infine segnaliamo che recentemente è stato dimostrato da A. Sathaye (*On planar curves*, in "Amer. J. Math.", *99*, 1977, pp. 1105-1135) che "ogni curva affine irriducibile non singolare di genere $\leqslant 1$ è isomorfa ad una curva piana".

Il Teorema 5.6 è stato successivamente esteso da Murthy, il quale ha dimostrato [207] che "se A è un dominio noetheriano UFD di dimensione 3 (tale che ogni modulo proiettivo di rango 3 è libero) e se $\mathfrak{a}$ è un ideale di A il quale può essere generato localmente da r elementi, allora $\mathfrak{a}$ può essere generato (globalmente) da $r + 1$ elementi". Ne segue in particolare:

Teorema 5.11. *Se* C *è una curva di* $\mathbf{A}^3_k$[26] *localmente intersezione completa, allora l'ideale* $\mathcal{I}(C)$ *può essere generato da tre elementi.*

Per le curve non singolari vale un risultato piú generale (si veda [174]):

Teorema 5.12. *Se* C *è una curva non singolare (eventualmente riducibile) di* $\mathbf{A}^n_k$, *allora l'ideale* $\mathcal{I}(C)$ *può essere generato da* n *elementi.*

[25] Ciò è immediato se la curva ha genere zero, nel qual caso, in virtú di un risultato di W. Cunnea ("Ill. J. Math.", *8*, 1964, pp. 425-438), si ha (con le notazioni di 5.8): $A/\mathfrak{a} \cong S^{-1}k[T]$, essendo T un'indeterminata e S una parte moltiplicativa di $k[T]$, da cui la tesi (cfr. [11, (26.E) e (26.G) Esempio 3]).

[26] Essendo k un campo arbitrario. Segnaliamo inoltre che, in virtú di un classico risultato di Forster e Ramspott (1965) "ogni curva (liscia) analitica in $\mathbf{A}^3_{\mathbf{C}}$ è un'intersezione completa (in senso stretto)".

Riguardo alle varietà in generale, fin dal 1964, O. Forster aveva enunciato [171] una congettura, la quale può venire espressa (in termini geometrici) nel modo seguente:

Congettura. L'ideale associato ad una qualsiasi varietà algebrica non singolare in $\mathbf{A}^n$ può essere generato da n elementi.[27]

Ebbene, la validità di tale congettura è stata dimostrata recentemente, come conseguenza di risultati algebrici più generali (cfr. [208]), da Sathaye e in pari tempo, con ipotesi meno restrittive, da Mohan Kumar (per un'ulteriore generalizzazione, si veda [219]). Precisamente, Mohan Kumar ha dimostrato il risultato seguente (cfr. [205]):

Teorema 5.13. *Sia k un campo oppure un dominio a ideali principali e sia $A = k[X_1, \ldots, X_n]$. Sia $\mathfrak{a}$ un ideale di A localmente intersezione completa. Allora $\mathfrak{a}$ è generato da* dim *A elementi.*

Il caso "debole"

Passiamo ora a considerare le varietà algebriche intersezioni complete in senso insiemistico (Def. 5.3).[28] Il risultato più importante ottenuto in tale ambito è dovuto a Ferrand e Szpiro (cfr. l'esposizione di Murthy in [24])[29]:

Teorema 5.14. *Ogni curva irriducibile localmente intersezione completa (in particolare, non singolare) di $\mathbf{A}^3_k$, essendo k un campo algebricamente chiuso arbitrario, è un'intersezione completa in senso insiemistico.*

Tale risultato (che è stato successivamente generalizzato da Mohan Kumar [205, Coroll. 5]) conduce, in modo naturale, a formulare due problemi distinti:

Problema 1. È possibile estendere il Teorema 5.14 ad una curva arbitraria di $\mathbf{A}^3_k$?

[27] Tale congettura è senz'altro vera per $n \leqslant 2$ e per varietà algebriche non singolari di dimensione $\leqslant 1$ (cfr. [174]). Essa è vera altresì [171] sostituendo "n" con "$n + 1$".

[28] È chiaro che ogni varietà intersezione completa (in senso stretto) lo è anche in senso insiemistico, mentre il viceversa non è vero in generale; tuttavia è possibile introdurre un'altra nozione di varietà intersezione completa (per una discussione in proposito, cfr. [216]).

[29] In esso si utilizza la validità della Congettura di Serre (per gli anelli di polinomi in tre variabili).

Problema 2. È possibile estendere il Teorema 5.14 ad un'arbitraria varietà di $\mathbf{A}_k^n$ che sia localmente intersezione completa?[30]

Per quanto riguarda il Problema 1, è stata data recentemente una risposta affermativa, per ogni campo k infinito di caratteristica $p > 0$, da Cowsik e Nori in [157] (cfr. anche [170]).

Riguardo al Problema 2 ci limitiamo a segnalare alcuni risultati parziali ottenuti da Murthy in [24] e alcuni risultati recenti di Boratynski, tra cui il seguente [142]:

Teorema 5.15. *Sia V una varietà di $\mathbf{A}_k^n$ e sia $\mathfrak{a} = \mathcal{I}(V)$ l'ideale associato a V in $A = k[X_1, \ldots, X_n]$. Supponiamo che:*

i) *V è localmente intersezione completa;*

ii) *$\mathfrak{a}/\mathfrak{a}^2$ è libero come $A/\mathfrak{a}$-modulo.*

Allora V risulta un'intersezione completa in senso insiemistico.

Prendendo lo spunto dal teorema precedente, conviene sottolineare che recentemente è stato approfondito ad opera di vari autori (tra cui, in primo luogo, Boratynski, Mohan Kumar e Vasconcelos) lo studio del cosiddetto "fibrato conormale" di un ideale $\mathfrak{a}$ di un anello noetheriano A, ossia del gruppo $\mathfrak{a}/\mathfrak{a}^2$ considerato come $A/\mathfrak{a}$-modulo; tale studio è stato poi utilizzato per affrontare il problema delle intersezioni complete, sia dal punto di vista "locale" che "globale".

Per finire, enunciamo due risultati dovuti rispettivamente a Boratynski e a Mohan Kumar. Il primo fornisce una generalizzazione della classica argomentazione di Serre (Teorema 5.6):

Proposizione 5.16. *Sia $\mathfrak{a}$ un ideale di un anello noetheriano tale che $\mu(\mathfrak{a}/\mathfrak{a}^2) \leq 2$. Allora esiste un modulo proiettivo di rango 2, diciamo P, ed un epimorfismo $P \twoheadrightarrow \mathfrak{a}$. In particolare, se P è libero, allora $\mathfrak{a}$ è generato da due elementi.*

Il secondo stabilisce alcuni legami tra ideali con fibrato conormale banale e varietà intersezioni complete (in senso stretto) [205]:

Proposizione 5.17. *Sia $A = k[X_1, \ldots, X_n]$, essendo k un campo*[31] *e sia $\mathfrak{a}$ un ideale di A tale che $\mathfrak{a}/\mathfrak{a}^2$ è libero come $A/\mathfrak{a}$-modulo. Allora, se si ha:* $\operatorname{ht}\mathfrak{a} \geqslant \dim A/\mathfrak{a} + 2$, *$\mathfrak{a}$ risulta un ideale intersezione completa.*

[30] Si noti che non è difficile dare esempi di superfici irriducibili (singolari) di $\mathbf{A}^4$ che non sono intersezioni complete in senso insiemistico (cfr. [178]).

[31] Oppure un dominio a ideali principali.

I problemi nell'ambiente proiettivo

Finora ci siamo limitati a considerare le varietà intersezioni complete (in senso stretto e in senso insiemistico) di uno spazio affine $\mathbf{A}^n_k$. Ebbene, passando all'ambiente proiettivo, ci si accorge subito che i problemi in esame sono alquanto più complicati, rispetto agli analoghi problemi studiati nel caso affine:

(1) È chiaro innanzitutto che lo spazio proiettivo è strutturalmente più "rigido" dello spazio affine: basta considerare il Teorema di Bézout o il fatto che non è più possibile (come nel caso affine) far "sparire" qualche intersezione residua all'infinito (cfr. 5.5 (1)).

(2) È subito visto (cfr. 5.5 (1)) che il Corollario 5.9 non si estende alle curve di $\mathbf{P}^3_k$. In generale, resta tuttora aperto il problema seguente, che risale addirittura a Kronecker e Cayley:

Problema. È vero che ogni curva irriducibile[32] di $\mathbf{P}^3$ è un'intersezione completa in senso insiemistico?[33]

Nel 1960, M. Kneser dimostrò che ogni curva irriducibile di $\mathbf{P}^3_{\mathbf{C}}$ è intersezione (in senso insiemistico) di tre superfici, e successivamente D. Eisenbud e G. Evans, completando alcuni risultati parziali di B. Segre e di U. Storch, provarono il risultato generale seguente [165]:

Teorema 5.18. *Sia V una varietà (non necessariamente pura) di uno spazio affine o proiettivo di dimensione n su un campo k algebricamente chiuso*[34] *e sia $\mathfrak{a} = \mathcal{I}(V)$ l'ideale associato a V. Allora $\mathfrak{a}$ è il radicale di un ideale generato da n elementi, ossia V è intersezione (in senso insiemistico) di al più n ipersuperfici.*[35]

[32] Si noti che ogni curva intersezione completa in senso insiemistico in $\mathbf{P}^3$ è necessariamente connessa [174, p. 235]. Ciò non è più vero nel caso affine: infatti (cfr. M. P. Murthy-J. Towber, *Algebraic vector bundles over* $\mathbf{A}^3$ *are trivial*, in "Inventiones Math.", *24*, 1974, pp. 173-189) "una curva riducibile in $\mathbf{A}^3$ è un'intersezione completa in senso insiemistico $\Leftrightarrow$ tali risultano le sue componenti connesse". Dunque, a differenza di ciò che accade in $\mathbf{P}^3$, una coppia di rette sghembe in $\mathbf{A}^3$ è *un'intersezione completa in senso insiemistico.*

[33] Cfr. anche [180]. È noto d'altra parte che esistono superfici irriducibili di $\mathbf{P}^4_{\mathbf{C}}$ che non sono intersezioni complete in senso insiemistico (cfr. [178]).

[34] Si noti che nel caso affine, l'enunciato è vero per un campo k qualsiasi, mentre nel caso proiettivo sembra necessario imporre delle restrizioni su k (in ogni caso, è sufficiente supporre k algebricamente chiuso).

[35] Già nel 1882 Kronecker aveva dimostrato in [193] un risultato analogo, facendo intervenire $n + 1$ ipersuperfici (di uno spazio di dimensione n). Per una breve storia dei tentativi per "abbassare" ad n tale limite, cfr. [165] oppure [174].

(3) Il Teorema 5.11 non continua piú a valere per le curve di $\mathbf{P}^3$. Piú precisamente, Geyer ha dimostrato in [174] che "per ogni numero naturale m, esiste una curva (irriducibile) non singolare in $\mathbf{P}^3$ tale che l'ideale ad essa associato non può essere generato da m elementi".

Tuttavia occorre aggiungere che, accanto alle difficoltà sopra accennate, si presenta spontaneamente un fenomeno, peculiare dell'ambiente proiettivo, il quale consente di semplificare notevolmente svariate questioni; in breve "le questioni relative ai problemi di intersezione completa hanno un carattere locale".

Si tratta precisamente del fatto che, se V è una varietà in $\mathbf{P}^n_k$ (con k alg. chiuso) e $\mathfrak{a} = \mathscr{I}(V)$ è l'ideale omogeneo associato a V in $A = k[X_0, \ldots, X_n]$, allora, posto $\mathfrak{m} = (X_0, \ldots, X_n)$, sicché $\mathfrak{a} \neq \mathfrak{m}$, si ha: $\mu(\mathfrak{a}) = \mu(\mathfrak{a}_\mathfrak{m})$.

Infatti, è chiaro che $\mu(\mathfrak{a}) \geqslant \mu(\mathfrak{a}_\mathfrak{m})$. Viceversa, sia $g_1, \ldots, g_s$ un sistema di generatori per $\mathfrak{a}_\mathfrak{m}$ e supponiamo (ciò che non è restrittivo) che $g_1, \ldots, g_s \in \mathfrak{a}$, e sia f un polinomio omogeneo di $\mathfrak{a}$; si ha allora una relazione della forma:

$$b \cdot f = \sum_{i=1}^{s} a_i g_i, \text{ con } b, a_i \in A, b \notin \mathfrak{m},$$

da cui, uguagliando i termini di grado minimo in ambo i membri, segue che $f \in (g_1, \ldots, g_s)$, ossia, data l'arbitrarietà di f: $\mu(\mathfrak{a}_\mathfrak{m}) \geqslant \mu(\mathfrak{a})$.[36]

Alla luce dell'osservazione ora sviluppata, è chiaro che, nello studio dei problemi di intersezione completa nell'ambiente proiettivo non vi è alcuna difficoltà nell'uso di tecniche e risultati riguardanti i moduli proiettivi.[37] In particolare, poggiando su un risultato analogo al Teorema 5.6, si ottiene [235, Par. 8] una caratterizzazione delle curve irriducibili non singolari di $\mathbf{P}^3$ che sono intersezioni complete, già dimostrata (per altra via) da G. Gherardelli ("Atti R. Acc. Italia", *4*, 1942, pp. 128-132):

Teorema 5.19. *Una curva irriducibile non singolare C di $\mathbf{P}^3$ è un'intersezione completa $\Leftrightarrow$ C è una curva di prima specie (nel senso di Dubreil) e la serie canonica di C è un multiplo della serie delle sezioni piane.*[38]

[36] Qui gioca in modo essenziale il fatto che $\mathfrak{a}$ è un ideale omogeneo.

[37] Infatti, per i moduli di tipo finito (su un anello arbitrario) la proiettività è una proprietà di carattere locale [3, Ch. 2].

[38] Notiamo che dire che C è una curva di prima specie, nel senso di Dubreil (cfr. [233]), equivale a dire che pd $\mathscr{I}(C) = 1$, mentre l'altra condizione si esprime anche (per $g > 1$) dicendo che le superfici di $\mathbf{P}^3$ di un certo ordine $d > 1$ segano su C divisori canonici, sicché si ha: $2g - 2 = d \cdot \deg C$, dove g e $\deg C$ denotano rispettivamente il genere e il grado (o ordine) di C.

Corollario 5.20. *Sia C una curva irriducibile non singolare di $\mathbf{P}^3$. Allora:*

i) *se C è razionale, C è un'intersezione completa $\Leftrightarrow$ C è una curva piana (ossia, è una retta oppure una conica);*

ii) *se C ha genere 2 (e non è piana), allora C non è mai un'intersezione completa.*

Si è già visto nella sezione 4 che la cubica sghemba di $\mathbf{P}^3$ è una varietà perfetta (4.2); inoltre essa è chiaramente una varietà "determinantale", giacché l'ideale ad essa associato può essere descritto come ideale generato dai determinanti dei minori di ordine 2 della matrice

$$\begin{pmatrix} X_0 & X_1 & X_2 \\ X_1 & X_2 & X_3 \end{pmatrix}^{39}$$

ed è chiaro che altrettanto può dirsi per la cubica sghemba di $\mathbf{A}^3$. Ebbene, piú in generale:

Proposizione 5.21. *Sia C una curva non singolare di $\mathbf{A}^3_k$ e sia $\mathfrak{a} = \mathcal{I}(C)$ l'ideale associato a C nell'anello $A = k[X_1, X_2, X_3]$, essendo k un campo algebricamente chiuso. Allora $\mathfrak{a}$ risulta un ideale perfetto generato dai determinanti dei minori di ordine 2 di una matrice 2×3 a elementi nell'anello A.*

Dimostrazione. Infatti osserviamo innanzitutto che $\mathfrak{a}$ è un ideale di altezza 2 in A, puro e localmente intersezione completa, sicché (5.7) pd $\mathfrak{a} \leqslant 1$; ne segue (cfr. [207]) che esiste una successione esatta corta della forma: $0 \to A^2 \to P \to \mathfrak{a} \to 0$, essendo P un A-modulo proiettivo (dunque libero), ossia[40] una successione esatta della forma:

$$0 \to A^2 \to A^3 \to \mathfrak{a} \to 0\,.$$

D'altra parte, si ha [6, p. 124, Th. B]: pd $A/\mathfrak{a} = 2$ e dunque, essendo A un anello di Cohen-Macaulay, $\mathfrak{a}$ risulta un ideale perfetto. A questo punto, la conclusione è immediata, in virtú del Teorema di Hilbert-Burch (cfr. [6, p. 148, Es. 8]).

Conviene aggiungere che la Proposizione 5.21 continua a valere in ipotesi alquanto piú generali (cfr. [216]).

[39] Segnaliamo inoltre che l'ideale della cubica sghemba di $\mathbf{P}^3$ è un'intersezione quasi-completa (un ideale $\mathfrak{a}$ di un anello noetheriano si dice un'*intersezione quasi completa*, se $\mu(\mathfrak{a}) \leqslant$ ht $\mathfrak{a} + 1$); per ulteriori proprietà di siffatti ideali, cfr. [227].

[40] Cfr. [6, p. 147, Es. 2].

Per finire, ci limitiamo a segnalare alcuni risultati recenti riguardanti le intersezioni complete ottenuti, nel caso delle varietà determinantali (affini o proiettive), da G. Valla in [244][41] e nel caso delle curve, da H. Bresinsky: *Monomial Gorenstein curves in* $\mathbf{A}^4$ *as set-theoretic complete intersections*, in "Manuscripta Math.", *27*, 1979, pp. 353-358 (si veda anche [183]).

Intersezioni complete e fattorialità

Un altro problema di grande interesse è quello delle cosiddette intersezioni complete "relative", ossia riferite ad una data varietà ambiente. Tale problema, enunciato e studiato sistematicamente[42] nella memoria di Andreotti e Salmon [131] consiste nello "studio delle varietà algebriche irriducibili V di uno spazio affine o proiettivo, tali che ogni sottovarietà di codimensione 1 di V sia un'intersezione completa di V con un'ipersuperficie dello spazio ambiente".

Si tratta di un problema che può definirsi "classico", giacché i primi risultati in proposito risalgono a circa un secolo fa, e precisamente a M. Noether e a F. Klein; esso tuttavia ha svolto un ruolo notevole nello sviluppo[43] dello studio di numerose questioni legate alla fattorialità, oltre che alle intersezioni complete, soprattutto a partire dal 1957, anno di pubblicazione della memoria sopra citata. Basti pensare ad esempio, ai lavori di P. Samuel,[44] al quale si deve anche la formulazione di talune congetture alquanto stimolanti, che hanno condotto a numerosi risultati di rilievo, tra cui il noto Teorema di Grothendieck, che citeremo piú avanti.

[41] Riportiamo in proposito l'enunciato di un notevole risultato di M. Hochster (non pubblicato): "Sia k un campo di caratteristica zero e siano $t < r < s$ interi positivi, e sia $A = k[X_{ij}]$ $(i = 1, \ldots, r,\ j = 1, \quad , s)$ l'anello dei polinomi in rs indeterminate. Allora l'ideale $I_t(X_{ij})$ generato dai determinanti dei minori di ordine t della matrice (X_{ij}) non è un'intersezione completa in senso insiemistico".

[42] Per la prima volta, fatta eccezione per una nota di Gröbner ("Rend. Mat.", *11*, 1952, pp. 217-223). Si veda anche: P. Salmon, *Sulla fattorialità delle algebre graduate e degli anelli locali*, in "Rend. Sem. Mat. Univ. Padova", *41*, 1968, pp. 119-138.

[43] Si consulti in proposito [23], [227], nonché l'esposizione contenuta in [104, pp. 531-546]. Occorre tuttavia citare, almeno di passaggio, i contributi di M. J. Bertin, V. I. Danilov, J. Lipman, M. P. Murthy, M. Nagata, P. Salmon, G. Scheja.

[44] Vedi nota precedente.

Prima di passare ad esaminare, sia pure rapidamente, alcuni risultati notevoli nel caso proiettivo, cominciamo con l'osservare che il problema in questione ammette, nel caso affine, una traduzione algebrica estremamente semplice (in virtú del Teorema dell'ideale principale di Krull):

Teorema 5.22. *Una varietà irriducibile e normale V di $\mathbf{A}^n_k$ (essendo k un campo algebricamente chiuso) gode della proprietà che ogni sua sottovarietà di codimensione* 1 *è un'intersezione completa di V con un'ipersuperficie di $\mathbf{A}^n_k \Leftrightarrow$ l'anello delle coordinate di V è un* UFD.[45]

Osservazione 5.23. Conviene notare esplicitamente che (cfr. ad es. [23, Prop. 10.2]) il Teorema 5.22 continua a valere per una varietà proiettiva che sia *proiettivamente normale*, ossia tale che il suo anello delle coordinate omogenee sia integralmente chiuso.

Riassumiamo ora in un unico enunciato i piú importanti risultati classici ottenuti nel caso proiettivo, insieme al risultato principale dimostrato in [131]:

Teorema 5.24. *Sia V una varietà proiettiva irriducibile soddisfacente ad una delle seguenti condizioni*:

(a) *V è una superficie "generica"*[46] *di $\mathbf{P}^3_{\mathbf{C}}$ di ordine $m \geqslant 4$*[47] (M. Noether, 1882)[48];

(b) *V è una quadrica non singolare di $\mathbf{P}^n_{\mathbf{C}}$, con $n \geqslant 4$* (Klein, 1883)[49];

(c) *V è un'ipersuperficie non singolare di $\mathbf{P}^n_{\mathbf{C}}$, con $n \geqslant 4$* (Severi, 1906);

(d) *V è una varietà intersezione completa, non singolare e di dimensione $\geqslant 3$, in $\mathbf{P}^n_{\mathbf{C}}$ (con $n \geqslant 4$)* (Lefschetz, 1921);

[45] È noto (cfr. il lavoro citato nella nota 25 precedente) che "una curva affine è tale che il suo anello delle coordinate è un UFD $\Leftrightarrow$ è razionale non singolare". Una generalizzazione di tale risultato è stata data da J. Hornell ("Proc. Amer. Math. Soc.", *53*, 1975, pp. 45-50).

[46] Per una precisazione di tale termine (che include senz'altro la non singolarità), cfr. ad es. [131].

[47] Tale ipotesi è necessaria, poiché [123, p. 65] ogni superficie di ordine $\leqslant 3$ contiene almeno una retta.

[48] Si veda, per un risultato collegato al Teorema di Noether: L. Robbiano, *A problem of complete intersections*, in "Nagoya Math. J.", *52*, 1973, pp. 129-132.

[49] Tale risultato è stato esteso largamente da M. Nagata (*A remark on the unique factorization theorem*, in "J. Math. Soc. Japan", *9*, 1957, pp. 143-145).

(e) *V è un'ipersuperficie di $\mathbf{P}_k^n$, con $n \geq 4$ e k campo algebricamente chiuso di caratteristica zero, eventualmente singolare, con luogo singolare di dimensione* $< n - 4$ (Andreotti-Salmon, 1957).

Allora ogni sottovarietà di codimensione 1 di V è un'intersezione completa di V con un'ipersuperficie dello spazio ambiente.

Ebbene, poggiando sul risultato 5.24 (e), Samuel[60] congetturò un risultato piú generale, il quale fu dimostrato subito dopo da A. Grothendieck (*Cohomologie locale des faisceaux cohérents et Théorèmes de Lefschetz locaux et globaux* (S.G.A. 2), Exposé XI, North Holland, 1968):

Teorema 5.25. *Sia A un anello locale della forma $R/\mathfrak{a}$, dove R è un anello locale regolare e $\mathfrak{a}$ è un ideale primo generato da una R-successione. Allora, se per ogni ideale primo $\mathfrak{p}$ di A di altezza ≤ 3, $A_\mathfrak{p}$ è un* UFD, *A risulta un* UFD.[61]

Dal Teorema 5.25 discendono facilmente i risultati 5.24 (b), (c), (d), (e): ci limitiamo qui a dedurre il Teorema di Lefschetz (negli altri casi, basta ripetere un'argomentazione analoga).

Sia V una varietà soddisfacente alle ipotesi del Teorema 5.24 (d); allora [103, p. 188] V è proiettivamente normale, sicché per ottenere la tesi, basta far vedere [23, Cor. 10.3] che l'anello locale nell'origine del cono affine Σ che proietta V in $\mathbf{A}_k^{n+1}$ [62] (dall'origine) è un UFD. Ora, se denotiamo con A tale anello locale, A può scriversi nella forma [11, (1.I.2)]: $R/\mathfrak{a}$, dove $R = k[X_0, \ldots, X_n]_{(X_0, \ldots, X_n)}$ e $\mathfrak{a} = \mathscr{I}(V)R$, dove $\mathscr{I}(V)$ denota l'ideale associato a V: dunque siamo nelle ipotesi del Teorema di Grothendieck (5.25).[63]

Sia $\mathfrak{p}$ un arbitrario ideale primo di altezza ≤ 3 in A: esso corrisponde ad una ben determinata sottovarietà W di dimensione ≥ 1 del cono Σ, e sia $P = (\alpha_0, \ldots, \alpha_n)$ un punto semplice di W.[64] Si osserva ora che l'anello $A_\mathfrak{p}$ può essere riscritto nella forma $A(\Sigma)_{\bar{\mathfrak{p}}}$,[65] essendo $\bar{\mathfrak{p}}$ l'ideale primo di $A(\Sigma)$ che corrisponde a $\mathfrak{p}$ (ossia tale che

[60] P. Samuel, *Sur les anneaux factoriels*, in "Bull. Soc. Math. France", *89*, 1961, pp. 155-173.

[61] Di tale risultato non si conosce finora alcuna dimostrazione "puramente" algebrica (la dimostrazione originaria di Grothendieck è essenzialmente coomologica).

[62] Supponiamo $V \subset \mathbf{P}_k^n$, con k campo algebricamente chiuso arbitrario.

[63] Si noti che $\mathfrak{a}$ ha altezza $(n + 1) - (\dim V + 1)$ in R ed è generato da $n - \dim V$ elementi, sicché $\mathfrak{a}$ è generato da una successione regolare [11, (16.B)].

[64] È chiaro che l'origine è l'unico punto singolare del cono Σ.

[65] Denotiamo con $A(\Sigma)$ l'anello delle coordinate del cono Σ.

$\bar{\mathfrak{p}}A = \mathfrak{p}$), sicché $A_\mathfrak{p}$ può essere ottenuto anche come ulteriore localizzazione (rispetto a un opportuno ideale primo) dell'anello locale $A(\Sigma)_\mathfrak{q}$, dove $\mathfrak{q}$ denota l'ideale $(X_0 - \alpha_0, \ldots, X_n - \alpha_n)/\mathcal{I}(V)$. Ma l'anello $A(\Sigma)_\mathfrak{q}$ è un anello locale regolare, poiché P è un punto semplice; ne segue che $A_\mathfrak{p}$ è un UFD (3.31, 3.32), donde la conclusione, in virtú del Teorema 5.25.

Osservazione 5.26. Si noti che, alla luce del Teorema di Grothendieck, gli enunciati 5.24 (b), (c), (d), (e) valgono in generale per un campo algebricamente chiuso arbitrario: da esso tuttavia non è possibile far discendere il Teorema di Noether (5.24 (a))[56] per ragioni di dimensione.

Per finire, segnaliamo che un problema analogo a quello ora esaminato può essere enunciato, nel senso insiemistico: si tratta cioè dello studio delle varietà irriducibili V di uno spazio affine o proiettivo, tali che ogni sottovarietà di codimensione 1 di V sia un'intersezione completa, in senso insiemistico, di V con un'ipersuperficie dello spazio ambiente.

Tale studio, già effettuato in taluni casi notevoli dai geometri classici, ha ripreso nuovo vigore negli ultimi anni, grazie anche all'introduzione e allo studio di appropriati strumenti algebrici, i cosiddetti anelli semifattoriali (cfr. [237], [23]). Per una panoramica dei principali risultati ottenuti in tale ambito, cfr. [172] e [227].

[56] Segnaliamo che di tale teorema si conoscono numerose dimostrazioni dovute in particolare a Lefschetz, Franchetta, Andreotti e Salmon, Moishezon, e infine a Deligne e Grothendieck, i quali hanno esteso il risultato in questione in caratteristica $p > 0$.

Bibliografia

A CURA DI PAOLO MAROSCIA

Algebra commutativa (*testi di carattere generale*)

1. M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading (Mass.) 1969 (tr. it. *Introduzione all'algebra commutativa*, Feltrinelli, Milano 1980).
2. M. Auslander, D. Buchsbaum, *Groups, Rings, Modules*, Harper & Row, New York 1974.
3. N. Bourbaki, *Algèbre Commutative*, Capp. 1-7, Hermann, Paris (1961-1965).
4. N. Bourbaki, *Algèbre*, Capp. 1-3, Hermann, Paris 1970.
5. N. Jacobson, *Lectures in Abstract Algebra*, voll. I, II, III, Van Nostrand, Princeton (1951-1964).
6. I. Kaplansky, *Commutative Rings* (ed. riveduta), The University of Chicago Press, 1974.
7. J. T. Knight, *Commutative Algebra*, Cambridge Univ. Press, 1971.
8. W. Krull, *Idealtheorie*, Springer, Berlin 1935.
9. J. P. Lafon, *Algèbre Commutative* (*Langages géométrique et algébrique*), Hermann, Paris 1977.
10. S. Lang, *Algebra*, Addison-Wesley, Reading (Mass.) 1965.
11. H. Matsumura, *Commutative Algebra*, Benjamin, New York 1970.
12. M. Nagata, *Local Rings*, Interscience, New York 1962.
13. D. G. Northcott, *Ideal Theory*, Cambridge Univ. Press, 1953.
14. B. L. van der Waerden, *Modern Algebra*, Ungar, New York, vol. I (1953), vol II (1950).
15. O. Zariski, P. Samuel, *Commutative Algebra*, Van Nostrand, Princeton, vol. I (1958), vol. II (1960).

Algebra commutativa (*testi di carattere specialistico*)

16. E. Artin, *Geometric Algebra*, Interscience, New York 1957 (tr. it. *Algebra geometrica*, Feltrinelli, Milano 1968).
17. H. Bass, *Algebraic K-Theory*, Benjamin, New York 1968.

18. H. Bass, *Projective modules and symmetric algebras*, I.M.P.A., Rio de Janeiro 1978.
19. J. W. Brewer, E. A. Rutter (a cura di), *Conference on Commutative Algebra*, Lect. Notes Math., *311*, Springer, Berlin 1973.
20. J. Dieudonné, *Topics in Local Algebra*, Notre Dame Math. Lect., *10*, Univ. of Notre Dame Press, Indiana 1967.
21. O. Endler, *Valuation Theory*, Springer, Berlin 1972.
22. J. Fogarty, *Invariant Theory*, Benjamin, New York 1969.
23. R. M. Fossum, *The divisor class group of a Krull domain*, Springer, Berlin 1973.
24. A. V. Geramita (a cura di), *Conference on Commutative Algebra*, Queen's Papers in Math., *42*, Kingston (Ontario) 1975.
25. A. V. Geramita, C. Small, *Introduction to homological methods in commutative rings*, Queen's Papers in Math., *43*, Kingston (Ontario) 1976.
26. R. Gilmer, *Multiplicative Ideal Theory*, Dekker, New York 1972.
27. S. Greco, P. Salmon, *Topics in* $\mathfrak{m}$*-adic Topologies*, Springer, Berlin 1971.
28. J. Herzog, E. Kunz, *Der kanonische Modul eines Cohen-Macaulay Rings*, Lect. Notes Math., *238*, Springer, Berlin 1971.
29. M. Hochster, *Topics in the homological theory of Modules over Commutative Rings*, C.B.M.S. Reg. Conf. Series, *24*, Amer. Math. Soc., 1975.
30. B. Iversen, *Generic local structure of the morphisms in Commutative Algebra*, Lect. Notes Math. *310*, Springer, Berlin 1970.
31. I. Kaplansky, *Fields and Rings*, University of Chicago Press, 1969.
32. I. Kaplansky, *An introduction to Differential Algebra*, Hermann, Paris 1957.
33. M. A. Knus, M. Ojanguren, *Théorie de la Descente et Algèbres d'Azumaya*, Lect. Notes Math., *389*, Springer, Berlin 1974.
34. T. Y. Lam, *Serre's Conjecture*, Lect. Notes Math., *635*, Springer, Berlin 1978.
35. J. Lambek, *Lectures on Rings and Modules*, Chelsea, New York 1976.
36. M. D. Larsen, P. J. Mc Carthy, *Multiplicative theory of ideals*, Academic Press, New York 1971.
37. F. S. Macaulay, *Algebraic theory of modular systems*, Cambridge Univ. Press, 1916.
38. M. P. Malliavin (a cura di), *Séminaire d'Algèbre Paul Dubreil 1976-77*, Lect. Notes Math., *641*, Springer, Berlin 1978.
39. E. Matlis, *One-dimensional Cohen-Macaulay rings*, Lect. Notes Math., *327*, Springer, Berlin 1973.
40. B. R. McDonald, R. A. Morris (a cura di), *Ring Theory II*, Dekker, New York 1977.
41. J. Milnor, *Introduction to Algebraic K-Theory*, Princeton Univ. Press, 1971.
42. M. Nagata, *Lectures on the fourteenth problem of Hilbert*, Lectures on Math., *31*, Tata Institute, Bombay 1965.
43. D. G. Northcott, *Lessons on Rings, Modules and Multiplicities*, Cambridge Univ. Press, 1968.

44. M. Orzech, C. Small, *The Brauer group of commutative rings*, Dekker, New York 1975.
45. S. Raghavan, B. Singh, R. Sridharan, *Homological methods in Commutative Algebra*, Tata Inst. Fund. Res., Oxford Univ. Press, 1975.
46. L. J. Ratliff, *Chain conjectures in Ring Theory*, Lect. Notes Math., *647*, Springer, Berlin 1978.
47. M. Raynaud, *Anneaux locaux henséliens*, Lect. Notes Math., *169*, Springer, Berlin 1970.
48. P. Ribenboim, *Théorie des valuations*, Les Presses de l'Université de Montréal, 1964.
49. J. D. Sally, *Numbers of generators of ideals in local rings*, Dekker, New York 1978.
50. P. Samuel, *Anneaux factoriels*, Univ. São Paulo, 1963.
51. P. Samuel, *Lectures on unique factorization domains*, Lectures on Math., *30*, Tata Institute, Bombay 1964.
52. J. P. Serre, *Algèbre locale-Multiplicités*, Lect. Notes Math., *11*, Springer, Berlin 1965.
53. B. Stenström, *Rings of quotients*, Springer, Berlin 1975.
54. R. G. Swan, *Algebraic K-Theory*, Lect. Notes Math., *76*, Springer, Berlin 1968.
55. W. V. Vasconcelos, *Divisor theory in Module categories*, North-Holland, Amsterdam 1974.
56. W. V. Vasconcelos, *The rings of dimension two*, Dekker, New York 1977.

Algebra omologica

57. M. André, *Homologie des algèbres commutatives*, Springer, Berlin 1974.
58. I. Bucur, A. Deleanu, *Introduction to the theory of Categories and Functors*, Wiley-Interscience, London 1968.
59. H. Cartan, S. Eilenberg, *Homological Algebra*, Princeton Univ. Press, 1956.
60. R. Godement, *Topologie algébrique et théorie des faisceaux*, Hermann, Paris 1958.
61. T. H. Gulliksen, G. Levin, *Homology of local rings*, Queen's Papers in Math., *20*, Kingston (Ontario) 1969.
62. P. J. Hilton, U. Stammbach, *A course in Homological Algebra*, Springer, Berlin 1971.
63. S. T. Hu, *Introduction to Homological Algebra*, Holden-Day, San Francisco 1968.
64. J. Jans, *Rings and Homology*, Holt, Rinehart and Winston, New York 1964.
65. S. MacLane, *Homology*, Springer, Berlin 1963.
66. D. G. Northcott, *An introduction to Homological Algebra*, Cambridge Univ. Press, 1960.

67. D. G. NORTHCOTT, *Finite free resolutions*, Cambridge Univ. Press, 1976.
68. J. J. ROTMAN, *Notes on Homological Algebra*, Van Nostrand, New York 1970.
69. J. R. STROOKER, *Introduction to categories, homological algebra and sheaf cohomology*, Cambridge Univ. Press, 1978.

Teoria algebrica dei numeri

70. Z. I. BOREVICH, I. R. SHAFAREVICH, *Number Theory*, Academic Press, New York and London 1966.
71. J. W. S. CASSELS, A. FRÖHLICH, *Algebraic Number Theory*, Academic Press, London and New York 1967.
72. H. COHN, *A classical invitation to algebraic numbers and class fields* (con due appendici di O. TAUSSKY), Springer, Berlin 1978.
73. G. H. HARDY, E. M. WRIGHT, *An introduction to the theory of numbers*, Clarendon Press, Oxford 1965.
74. H. HASSE, *Number Theory*, Springer, Berlin 1978.
75. S. LANG, *Algebraic Number Theory*, Addison-Wesley, Reading (Mass.) 1970.
76. S. LANG, *Cyclotomic Fields*, Springer, Berlin 1978.
77. H. B. MANN, *Introduction to Algebraic Number Theory*, Columbus (Ohio) 1955.
78. P. RIBENBOIM, *Algebraic Numbers*, Wiley-Interscience, New York 1972.
79. P. RIBENBOIM, *L'arithmétique des corps*, Hermann, Paris 1974.
80. P. SAMUEL, *Théorie algébrique des nombres*, Hermann, Paris 1967.
81. J. P. SERRE, *Corps locaux*, Hermann, Paris 1962.
82. J. P. SERRE, *Cours d'arithmétique*, Presses Universitaires de France, Paris 1970.
83. A. WEIL, *Basic Number Theory*, 3 ed., Springer, Berlin 1974.
84. E. WEISS, *Algebraic Number Theory*, Mc Graw-Hill, New York 1963.

Geometria algebrica

85. S. S. ABHYANKAR, *Algebraic Space Curves*, Séminaire Math. Sup., *43*, Montréal 1971.
86. A. ALTMAN, S. KLEIMAN, *Introduction to Grothendieck Duality Theory*, Lect. Notes Math., *146*, Springer, Berlin 1970.
87. M. ARTIN, *Algebraic Spaces*, Yale Univ. Press, 1971.
88. M. BALDASSARRI, *Algebraic Varieties*, Springer, Berlin 1956.
89. A. BOREL, *Linear Algebraic Groups*, Benjamin, New York 1969.
90. J. F. BOUTOT, *Schéma de Picard local*, Lect. Notes Math., *632*, Springer, Berlin 1978
91. C. CHEVALLEY, *Introduction to the theory of algebraic functions in one variable*, Amer. Math. Soc., New York 1951.

92. M. Deuring, *Lectures on the theory of algebraic functions of one variable*, Lect. Notes Math., *314*, Springer, Berlin 1973.
93. J. Dieudonné, *Cours de géométrie algébrique*, voll. I, II, Presses Universitaires de France, 1974.
94. W. Fulton, *Algebraic Curves*, Benjamin, New York 1969.
95. S. Greco, *Normal Varieties*, Istituto Nazionale di Alta Matematica, Institutiones Mathematicae, vol. IV, Academic Press, London 1978.
96. P. Griffiths, J. Adams, *Topics in algebraic and analytic geometry*, Princeton Univ. Press, 1974.
97. P. Griffiths, J. Harris, *Principles of algebraic geometry*, Wiley, New York 1978.
98. W. Gröbner, *Moderne algebraische Geometrie*, Springer, Wien und Innsbruck 1949.
99. A. Grothendieck, *Local Cohomology*, Lect. Notes Math., *41*, Springer, Berlin 1967.
100. A. Grothendieck, J. Dieudonné, *Eléments de Géométrie Algébrique*, I, II, III, IV, I.H.E.S., Publ. Math., *4*, *8*, ..., Paris 1961 ....
101. A. Grothendieck, J. Dieudonné, *Eléments de Géométrie Algébrique*, I, Springer, Berlin 1971.
102. R. Hartshorne, *Ample subvarieties of algebraic varieties*, Lect. Notes Math., *156*, Springer, Berlin 1970.
103. R. Hartshorne, *Algebraic Geometry*, Springer, Berlin 1977.
104. R. Hartshorne (a cura di), *Algebraic Geometry* (Arcata 1974), Amer. Math. Soc. Proc. Symp. Pure Math., *29*, 1975.
105. J. E. Humphreys, *Linear Algebraic Groups*, Springer, Berlin 1975.
106. D. Knutson, *Algebraic Spaces*, Lect. Notes Math., *203*, Springer, Berlin 1971.
107. S. Lang, *Introduction to Algebraic Geometry*, Interscience, New York 1958.
108. K. Lønsted (a cura di), *Algebraic Geometry*, Lect. Notes Math., *732*, Springer, Berlin 1979.
109. I. G. Macdonald, *Algebraic Geometry*, Benjamin, New York 1968.
110. D. Mumford, *Geometric Invariant Theory*, Springer, Berlin 1965.
111. D. Mumford, *Introduction to Algebraic Geometry*, Harvard Lect. Notes, 1967.
112. D. Mumford, *Abelian Varieties*, Tata Inst. Fund. Res., Oxford Univ. Press, 1974.
113. D. Mumford, *Curves and their Jacobians*, Univ. of Michigan Press, 1975.
114. D. Mumford, *Algebraic Geometry*, I, Springer, Berlin 1976.
115. L. D. Olson (a cura di), *Algebraic Geometry*, Lect. Notes Math., *687*, Springer, Berlin 1978.
116. F. Oort, *Commutative group schemes*, Lect. Notes Math., *15*, Springer, Berlin 1966.
117. F. Oort (a cura di), *Algebraic Geometry* (Oslo 1970), Wolters-Noordhoff, Groningen 1972.

118. P. SAMUEL, *Lectures on old and new results on algebraic curves*, Lectures on Math., *36*, Tata Institute, Bombay 1966.
119. P. SAMUEL, *Méthodes d'algèbre abstraite en géométrie algébrique*, 2 ed., Springer, Berlin 1972.
120. B. SEGRE, *Prodromi di geometria algebrica* (con un'Appendice di U. BARTOCCI e M. LORENZANI), Cremonese, Roma 1972.
121. A. SEIDENBERG, *Elements of the theory of algebraic curves*, Addison-Wesley, Reading (Mass.) 1968.
122. J. P. SERRE, *Groupes algébriques et corps de classes*, Hermann, Paris 1959.
123. I. R. SHAFAREVICH, *Basic Algebraic Geometry*, Springer, Berlin 1974.
124. A. TOGNOLI, *Algebraic Geometry and Nash Functions*, Istituto Nazionale di Alta Matematica, Institutiones Mathematicae, vol. III, Academic Press, London 1978.
125. R. J. WALKER, *Algebraic Curves*, Princeton Univ. Press, 1950.
126. A. WEIL, *Foundations of Algebraic Geometry*, Amer. Math. Soc., New York 1946.
127. H. WEYL, *The classical groups*, Princeton Univ. Press, 1946.
128. O. ZARISKI, *An introduction to the theory of algebraic surfaces*, Lect. Notes Math., *83*, Springer, Berlin 1969.
129. O. ZARISKI, *Algebraic Surfaces*, 2 ed., Springer, Berlin 1971.

Articoli vari

130. S. S. ABHYANKAR, *Historical ramblings in algebraic geometry and related algebra*, in "Amer. Math. Monthly," *83*, 1976, pp. 409-448.
131. A. ANDREOTTI, P. SALMON, *Anelli con unica decomponibilità in fattori primi ed un problema di intersezioni complete*, in "Monatsh. für Math.," *61*, 1957, pp. 97-142.
132. E. ARTIN, *Zur Theorie der hypercomplexen Zahlen*, in "Abh. Math. Sem. Univ. Hamburg," *5*, 1927, pp. 251-260.
133. E. ARTIN, J. TATE, *A note on finite ring extensions*, in "J. of Math. Soc. of Japan," *3*, 1951, pp. 74-77.
134. M. ARTIN, M. NAGATA, *Residual intersections in Cohen-Macaulay rings*, in "J. Math. Kyoto Univ.," *12*, 1972, pp. 307-323.
135. M. AUSLANDER, D. BUCHSBAUM, *Homological dimension in local rings*, in "Trans. Amer. Math. Soc.," *85*, 1957, pp. 390-405.
136. M. AUSLANDER, D. BUCHSBAUM, *Codimension and multiplicity*, in "Ann. of Math.," *68*, 1958, pp. 625-657.
137. M. AUSLANDER, D. BUCHSBAUM, *Unique factorization in regular local rings*, in "Proc. Nat. Acad. Sci. USA," *45*, 1959, pp. 733-734.
138. M. AUSLANDER, O. GOLDMAN, *The Brauer group of a commutative ring*, in "Trans. Amer. Math. Soc.," *97*, 1960, pp. 367-409.
139. G. AZUMAYA, *On maximally central algebras*, in "Nagoya Math. J.," *2*, 1950, pp. 119-150.

140. H. BASS, *Injective dimension in Noetherian rings*, in "Trans. Amer. Math. Soc.," *102*, 1962, pp. 18-29.
141. H. BASS, *On the ubiquity of Gorenstein rings*, in "Math. Z.," *82*, 1963, pp. 8-28.
142. M. BORATYŃSKY, *A note on set-theoretic complete intersection ideals*, in "J. Algebra," *54*, 1978, pp. 1-5.
143. A. BOREL, J. P. SERRE, *Le théorème de Riemann-Roch* (da A. Grothendieck), in "Bull. Soc. Math. France," *86*, 1958, pp. 97-136.
144. D. BUCHSBAUM, D. EISENBUD, *What makes a complex exact?*, in "J. Algebra," *25*, 1973, pp. 259-268.
145. D. BUCHSBAUM, D. EISENBUD, *Some structure theorems for finite free resolutions*, in "Advances in Math.," *12*, 1974, pp. 84-139.
146. D. BUCHSBAUM, D. EISENBUD, *Generic free resolutions and a family of generically perfect ideals*, in "Advances in Math.," *18*, 1975, pp. 245-301.
147. D. BUCHSBAUM, D. EISENBUD, *Algebra structures for finite free resolutions and some structure theorems for ideals of codimension 3*, in "Amer. J. Math.," *99*, 1977, pp. 447-485.
148. D. BUCHSBAUM, *A new construction of the Eagon-Northcott complex*, in "Advances in Math.," *34*, 1979, pp. 58-76.
149. L. BURCH, *On ideals of finite homological dimension in local rings*, in "Proc. Camb. Phil. Soc.," *64*, 1968, pp. 941-948.
150. S. CHASE, D. HARRISON, A. ROSENBERG, *Galois theory and cohomology of commutative rings*, in "Mem. Amer. Math. Soc.," *52*, 1965.
151. C. CHEVALLEY, *On the theory of local rings*, in "Ann. of Math.," *44*, 1943, pp. 690-708.
152. C. CHEVALLEY, *Intersections of algebraic and algebroid varieties*, in "Trans. Amer. Math. Soc.," *57*, 1945, pp. 1-85.
153. L. CLABORN, *Every abelian group is a class group*, in "Pacific J. Math.," *18*, 1966, pp. 219-222.
154. I. S. COHEN, *On the structure and ideal theory of complete local rings*, in "Trans. Amer. Math. Soc.," *59*, 1946, pp. 54-106.
155. I. S. COHEN, *Rings with restricted minimum condition*, in "Duke Math. J.," *17*, 1950, pp. 27-42.
156. I. S. COHEN, A. SEIDENBERG, *Prime ideals and integral dependence*, in "Bull. Amer. Math. Soc.," *52*, 1946, pp. 252-261.
157. R. C. COWSIK, M. V. NORI, *Curves in characteristic p are set-theoretic complete intersections*, in "Inventiones Math.", *45*, 1978, pp. 111-114.
158. E. D. DAVIS, *On the geometric interpretation of seminormality*, in "Proc. Amer. Math. Soc.," *68*, 1978, pp. 1-5.
159. C. DE CONCINI, D. EISENBUD, C. PROCESI, *Young diagrams and determinantal varieties*, in "Inventiones Math.", *56*, 1980, pp. 129-165.
160. R. DEDEKIND, H. WEBER, *Theorie der algebraischen Funktionen einer Veränderlichen*, in "J. f. Math." (Crelle), *92*, 1882, pp. 181-290.
161. J. DIEUDONNÉ, *Algebraic Geometry*, in "Advances in Math.," *3*, 1969, pp. 233-321.

162. J. Dieudonné, *Fondements de la géométrie algébrique moderne*, in "Advances in Math.," *3*, 1969, pp. 322-413.
163. J. A. Eagon, D. G. Northcott, *Ideals defined by matrices and a certain complex associated with them*, in "Proc. Roy. Soc.," serie A, *269*, 1962, pp. 188-204.
164. P. M. Eakin, Jr. - W. J. Heinzer, *A cancellation problem for commutative rings*, Lect. Notes Math. *311*, Springer, Berlin 1973, pp. 61-77.
165. D. Eisenbud, E. G. Evans, *Every algebraic set in n-space is the intersection of n hypersurfaces*, in "Inventiones Math.," *19*, 1973, pp. 107-112.
166. D. Eisenbud, E. G. Evans, *Three conjectures about modules over polynomial rings*, Lect. Notes Math., *311*, Springer, Berlin 1973, pp. 78-89.
167. D. Eisenbud, *An algebraic approach to the topological degree of a smooth map*, in "Bull. Amer. Math. Soc.," *84*, 1978, pp. 751-764.
168. E. G. Evans, P. A. Griffith, *Local cohomology modules for normal domains*, in "J. London Math. Soc.," *19*, 1979, pp. 277-284.
169. D. Ferrand, *Courbes gauches et fibrés de rang deux*, in "C. R. Acad. Sci. Paris," *281*, 1975, pp. A345-A347.
170. D. Ferrand, *Set-theoretical complete intersections in characteristic $p > 0$*, Lect. Notes Math., *732*, Springer, Berlin 1979, pp. 82-89.
171. O. Forster, *Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring*, in "Math. Z.," *84*, 1964, pp. 80-87; Erratum, *ibid.*, *86*, 1964, p. 190.
172. D. Gallarati, *Intersezioni complete e contatto di superficie algebriche*, Bressanone 1979 (apparirà nei *Seminari dell'Ist. Mat. di Genova*).
173. A. V. Geramita, C. A. Weibel, *Principal ideals and smooth curves*, in "J. Algebra", *62*, 1980, pp. 235-248.
174. W. D. Geyer, *On the number of equations which are necessary to describe an algebraic set in n-space*, Atas III Escola de Algebra, Brasilia 1976, pp. 183-317.
175. S. Greco, N. Sankaran, *On the separable and algebraic closedness of a Hensel couple in its completion*, in "J. Algebra," *39*, 1976, pp. 335-348.
176. S. Greco, C. Traverso, *On seminormal schemes*, in "Compositio Math.", *40*, 1980, pp. 325-365.
177. A. Grothendieck, *Sur quelques points d'algèbre homologique*, in "Tôhoku Math. J.," *9*, 1957, pp. 119-221.
178. R. Hartshorne, *Complete intersections and connectedness*, in "Amer. J. Math.," *84*, 1962, pp. 497-508.
179. R. Hartshorne, *Varieties of small codimension in projective space*, in "Bull. Amer. Math. Soc.," *80*, 1974, pp. 1017-1032.
180. R. Hartshorne, *Complete intersections in characteristic $p > 0$*, in "Amer. J. Math.," *101*, 1979, pp. 380-383.
181. R. Hartshorne, *Algebraic vector bundles on projective spaces: a problem list*, in "Topology," *18*, 1979, pp. 117-128.
182. R. Hartshorne, A. Ogus, *On the factoriality of local rings of small embedding codimension*, in "Commun. in Alg.," *1*, 1974, pp. 415-437.

183. J. HERZOG, *Generators and relations of abelian semigroups and semigroup rings*, in "Manuscripta Math.," *3*, 1970, pp. 175-193.
184. D. HILBERT, *Über die Theorie der Algebraischen Formen*, in "Math. Ann.," *36*, 1890, pp. 473-534.
185. D. HILBERT, *Über die vollen Invariantensysteme*, in "Math. Ann.," *42*, 1893, pp. 313-373.
186. H. HIRONAKA, *Resolution of singularities of an algebraic variety over a field of characteristic zero*, in "Ann. of Math.," *79*, 1964, I: pp. 109-203; II: pp. 205-326.
187. M. HOCHSTER, *Prime ideal structure in commutative rings*, in "Trans. Amer. Math. Soc.," *142*, 1969, pp. 43-60.
188. M. HOCHSTER, *Criteria for equality of ordinary and symbolic powers of primes*, in "Math. Z.," *133*, 1973, pp. 53-65.
189. M. HOCHSTER, *Grassmannians and their Schubert varieties are arithmetically Cohen-Macaulay*, in "J. Algebra", *25*, 1973, pp. 40-57.
190. M. HOCHSTER, J. A. EAGON, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, in "Amer. J. Math.," *93*, 1971, pp. 1020-1058.
191. M. HOCHSTER, J. L. ROBERTS, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, in "Advances in Math.," *13*, 1974, pp. 115-175.
192. J. IGUSA, *On the arithmetic normality of the Grassmann variety*, in "Proc. Nat. Acad. Sc. USA," *40*, 1954, pp. 309-313.
193. L. KRONECKER, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, in "J. Reine Angew. Math.," *92*, 1882, pp. 1-123.
194. W. KRULL, *Primidealketten in allgemeinen Ringbereichen*, S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl., *7*, 1928.
195. W. KRULL, *Allgemeine Bewertungstheorie*, in "J. Reine Angew. Math.," *167*, 1931, pp. 160-196.
196. W. KRULL, *Dimensionstheorie in Stellenringen*, in "J. Reine Angew. Math.," *179*, 1938, pp. 204-226.
197. W. KRULL, *Jacobsonsche Ringe, Hilbertscher Nullstellensatz, Dimensionstheorie*, in "Math. Z.," *54*, 1951, pp. 354-387.
198. A. LASCOUX, *Syzygies des variétés déterminantales*, in "Advances in Math.," *30*, 1978, pp. 202-237.
199. E. LASKER *Zur Theorie der Moduln und Ideale*, in "Math. Ann.," *60*, 1905, pp. 20-116.
200. D. LAZARD, *Autour de la platitude*, in "Bull. Soc. Math. France," *97*, 1969, pp. 81-128.
201. S. LICHTENBAUM, M. SCHLESSINGER, *The cotangent complex of a morphism*, in "Trans. Amer. Math. Soc.," *128*, 1967, pp. 41-70.
202. J. LIPMAN, *Introduction to resolution of singularities*, in *Algebraic Geometry* (Arcata 1974), Amer. Math. Soc. Proc. Symp. Pure Math., *29*, 1975, pp. 187-230.
203. J. LIPMAN, *Rings with discrete divisor class group: Theorem of Danilov-Samuel*, in "Amer. J. Math.," *101*, 1979, pp. 203-211.

204. R. MAC RAE, *On an application of the Fitting invariants*, in "J. Algebra," *2*, 1965, pp. 153-169.
205. N. MOHAN KUMAR, *On two conjectures about polynomial rings*, in "Inventiones Math.," *46*, 1978, pp. 225-236.
206. M. P. MURTHY, *A note on factorial rings*, in "Archiv der Math.," *15*, 1964, pp. 418-420.
207. M. P. MURTHY, *Generators for certain ideals in regular rings of dimension three*, in "Comment. Math. Helv.," *47*, 1972, pp. 179-184.
208. M. P. MURTHY, *Affine varieties as complete intersections*, in "Proc. Internat. Symp. on Algebraic Geometry" (Kyoto 1977), pp. 231-236.
209. M. P. MURTHY, R. G. SWAN, *Vector bundles over affine surfaces*, in "Inventiones Math.," *36*, 1976, pp. 125-165.
210. M. NAGATA, *The theory of multiplicity in general local rings*, in "Proc. Internat. Symp. Algebraic Number Theory" (Tokyo 1955), pp. 191-226.
211. M. NAGATA, *On the chain problem of prime ideals*, in "Nagoya Math. J.," *10*, 1956, pp. 51-64.
212. M. NAGATA, *On the closedness of singular loci*, I.H.E.S., Publ. Math., *2*, Paris 1959, pp. 29-36.
213. E. NOETHER, *Idealtheorie in Ringbereichen*, in "Math. Ann.," *83*, 1921, pp. 24-66.
214. E. NOETHER, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p*, Nachr. Ges. Wiss. Göttingen, 1926, pp. 28-35.
215. E. NOETHER, *Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern*, in "Math. Ann.," *96*, 1927, pp. 26-61.
216. J. OHM, *Space curves as ideal-theoretic complete intersections* (preprint).
217. C. PESKINE, L. SZPIRO, *Dimension projective finie et cohomologie locale*, I.H.E.S., Publ. Math., *42*, Paris 1973, pp. 323-395.
218. C. PESKINE, L. SZPIRO, *Liaison des variétés algébriques*, I, in "Inventiones Math.", *26*, 1974, pp. 271-302.
219. B. R. PLUMSTEAD, *The conjectures of Eisenbud and Evans* (tesi di dottorato), The University of Chicago, 1979.
220. C. PROCESI, *Young diagrams, standard monomials and invariant theory*, in "Proc. Internat. Congress Math.," Helsinki 1978.
221. D. QUILLEN, *Projective modules over polynomial rings*, in "Inventiones Math.," *36*, 1976, pp. 167-171.
222. M. RAYNAUD, L. GRUSON, *Critères de platitude et de projectivité*, in "Inventiones Math.," *13*, 1971, pp. 1-89.
223. D. REES, *The grade of an ideal or module*, in "Proc. Camb. Phil. Soc.," *53*, 1957, pp. 28-42.
224. D. REES, *A note on analytically unramified local rings*, in "J. London Math. Soc.," *36*, 1961, pp. 24-28.
225. P. SALMON, *Metodi omologici in algebra commutativa*, in "Boll. Un. Mat. Ital.," *7*, suppl. fasc. 1, 1973, pp. 10-17.

226. P. SALMON, *Applicazioni della K-teoria algebrica all'algebra commutativa*, in *Categories and Commutative Algebra*, Cremonese, Roma 1973, pp. 213-247.
227. P. SALMON, *Intersezioni complete e loro generalizzazioni*, Ist. Naz. di Alta Matematica, Roma 1979 (apparirà sui "Symposia Mathematica").
228. P. SAMUEL, *La notion de multiplicité en algèbre et en géométrie algébrique*, in "J. math. pures et appl.," *30*, 1951, pp. 159-274.
229. P. SAMUEL, *Algèbre locale*, in "Mém. Sci. Math.," *123*, Paris 1953.
230. A. SEIDENBERG, *A note on the dimension theory of rings*, in "Pacific J. Math.," *3*, 1953, pp. 505-512.
231. A. SEIDENBERG, *On the dimension theory of rings*, II, in "Pacific J. Math.," *4*, 1954, pp. 603-614.
232. J. P. SERRE, *Géométrie algébrique et géométrie analytique*, in "Ann. Inst. Fourier," *6*, 1955, pp. 1-42.
233. J. P. SERRE, *Faisceaux algébriques cohérents*, in "Ann. of Math.," *61*, 1955, pp. 197-278.
234. J. P. SERRE, *Sur la dimension homologique des anneaux et des modules noethériens*, in "Proc. Internat. Symp. Algebraic Number Theory," Tokyo 1955, pp. 175-189.
235. J. P. SERRE, *Sur les modules projectifs*, in "Sém. Dubreil-Pisot," 1960-1961.
236. R. STANLEY, *Hilbert functions of graded algebras*, in "Advances in Math.," *28*, 1978, pp. 57-83.
237. U. STORCH, *Fastfaktorielle Ringe*, in "Schriftenreihe Math. Inst. Univ. Münster," Quaderno *36*, 1967.
238. A. A. SUSLIN, *Projective modules over a polynomial ring are free*, in "Soviet Math. Dokl.," *17*, 1976, pp. 1160-1164.
239. R. G. SWAN, *Vector bundles and projective modules*, in "Trans. Amer. Math. Soc.," *105*, 1962, pp. 264-277.
240. R. G. SWAN, *The number of generators of a module*, in "Math. Z.," *102*, 1967, pp. 318-322.
241. J. TATE, *Homology of Noetherian rings and local rings*, in "Ill. J. Math.," *1*, 1957, pp. 14-27.
242. C. TRAVERSO, *Seminormality and Picard group*, in "Ann. Scuola Norm. Sup. Pisa," *24*, 1970, pp. 585-595.
243. P. VALABREGA, *On the excellence property for power series rings over polynomial rings*, in "J. Math. Kyoto Univ.," *15*, 1975, pp. 387-395.
244. G. VALLA, *On determinantal ideals which are set-theoretic complete intersections*, in "Compositio Math." (in corso di stampa).
245. W. V. VASCONCELOS, *Ideals generated by R-sequences*, in "J. Algebra," *6*, 1967, pp. 309-316.
246. J. M. WAHL, *Equations defining rational singularities*, in "Ann. Scient. Éc. Norm. Sup.," *10*, 1977, pp. 231-264.
247. O. ZARISKI, *Generalized semilocal rings*, in "Summa Brasil. Math.," *1*, 1946, pp. 169-195.

248. O. ZARISKI, *The concept of a simple point of an abstract algebraic variety*, in "Trans. Amer. Math. Soc.," *62*, 1947, pp. 1-52.
249. O. ZARISKI, *Analytical irreducibility of normal varieties*, in "Ann. of Math.," *49*, 1948, pp. 352-361.
250. O. ZARISKI, *Sur la normalité analytique des variétés normales*, in "Ann. Inst. Fourier," *2*, 1950, pp. 161-164.
251. D. ZELINSKY, *Brauer groups*, in *Ring Theory II*, Dekker, New York 1977, pp. 69-101.

Collana di matematica
diretta da Lucio Lombardo Radice ed Edoardo Vesentini

Guido Zappa, Rodolfo Permutti, *Gruppi corpi equazioni*

Claude Chevalley, *Concetti fondamentali di algebra. Costruzione e studio di alcune importanti algebre*
Trad. di Maria Luisa Vesentini Ottolenghi

Lucio Lombardo Radice, *Istituzioni di algebra astratta*
Edizione riveduta
Esercizi e complementi a cura di V. Corbas e G. Panella

Marc Zamansky, *Introduzione all'algebra e all'analisi moderna*
Trad. di Luigi Muracchini

V. Checcucci, A. Tognoli, E. Vesentini, *Lezioni di topologia generale*

Emil Artin, *Algebra geometrica*
Trad. di Lucio Lombardo Radice e Gianfranco Panella

Paul R. Halmos, *Teoria elementare degli insiemi*
Trad. di Maria Luisa Vesentini Ottolenghi ed Edoardo Vesentini

P.M. Cohn, *Algebra universale*
Trad. di Maurizio Fattorosi Barnaba

Alexander Abian, *La teoria degli insiemi e l'aritmetica transfinita*
Trad. di Giulia Maria Piacentini Cattaneo

Paul J. Cohen, *La teoria degli insiemi e l'ipotesi del continuo*
Appendice all'edizione italiana e trad. di Gabriele Lolli

Antonio Machì, *Introduzione alla teoria dei gruppi*

M. Girardi, G. Israel, *Teoria dei campi*

Franco Banino, *Geometria per fisici*

Ferenc Kárteszi, *Introduzione alle geometrie finite*
Trad. di Simona Panattoni

Filosofia della scienza

collana diretta da Ludovico Geymonat

1 Willard Van Orman Quine, *Manuale di logica*
Introduzione di M. Pacifico
2 Ettore Casari, *Lineamenti di logica matematica*
3 Ludovico Geymonat, *Filosofia e filosofia della scienza*
4 Carl G. Hempel, *La formazione dei concetti e delle teorie nella scienza empirica*
Cura e prefazione di A. Pasquinelli
5 Evert W. Beth, *I fondamenti logici della matematica*
Cura e prefazione di E. Casari
6 Ettore Casari, *Questioni di filosofia della matematica*
7 Alberto Pasquinelli, *Nuovi principi di epistemologia*
8 Richard Bevan Braithwaite, *La spiegazione scientifica. Uno studio sulla funzione della teoria, della probabilità delle leggi nella scienza*
Cura e prefazione di G. Jesurum
9 Ernest Nagel, *La struttura della scienza. Problemi di logica della spiegazione scientifica*
Prefazione di A. Monti
10 Maria Luisa dalla Chiara Scabia, *Modelli sintattici e semantici delle teorie elementari*
11 Domenico Costantini, *Fondamenti del calcolo delle probabilità*
12 Emil Ungerer, *Fondamenti teorici delle scienze biologiche*
Cura e introduzione di F. Mondella
13 M.E. Omelyanovskij, V.A. Fock e altri, *L'interpretazione della meccanica quantistica. Fisica e filosofia in URSS*
Cura di S. Tagliagambe. Prefazione di L. Geymonat
14 Enrico Bellone, *I modelli e la concezione del mondo nella fisica moderna. Da Laplace a Bohr*
15 Imre Lakatos e Alan Musgrave (a cura di), *Critica e crescita della conoscenza*
Cura e introduzione all'edizione italiana di G. Giorello
16 Hans Reichenbach, *Filosofia dello spazio e del tempo*
Osservazioni introduttive di R. Carnap. Prefazione all'edizione italiana di L. Geymonat. Nota bibliografica di A. Carugo
17 Ludovico Geymonat, *Scienza e realismo*
18 Pietro Redondi, *Epistemologia e storia della scienza*
19 Imre Lakatos, *Dimostrazioni e confutazioni. La logica della scoperta matematica*
Cura e prefazione di J. Worrall e E. Zahar. Cura e introduzione all'edizione italiana di G. Giorello
20 Mary B. Hesse, *Modelli e analogie nella scienza*
Edizione italiana a cura di Cristina Bicchieri

Storia della scienza

collana impostata da Paolo Rossi e Libero Sosio

Marie Boas, *Il Rinascimento scientifico 1450/1630*
Introduzione di A. R. Hall
Marshall Clagett, *La scienza della meccanica nel Medioevo*
Alistair C. Crombie, *Da S. Agostino a Galileo. Storia della scienza dal V al XVII secolo*
E. J. Dijksterhuis, *Il meccanicismo e l'immagine del mondo. Dai Presocratici a Newton*
J. L. E. Dreyer, *Storia dell'astronomia da Talete a Keplero*
Prefazione di W. H. Stahl
Loren Eiseley, *Il secolo di Darwin. L'evoluzione e gli uomini che la scoprirono*
Yehuda Elkana, *La scoperta della conservazione dell'energia*
Prefazione di I. B. Cohen
Bertrand Gille, *Leonardo e gli ingegneri del Rinascimento*
John C. Greene, *La morte di Adamo. L'evoluzionismo e la sua influenza sul pensiero occidentale*
A. Rupert Hall, *Da Galileo a Newton (1630/1720)*
— *La Rivoluzione scientifica 1500/1800. La formazione dell'atteggiamento scientifico moderno*
Mary B. Hesse, *Forze e campi. Il concetto di azione a distanza nella storia della fisica*
Max Jammer, *Storia del concetto di forza. Studio sulle fondazioni della dinamica*
— *Storia del concetto di massa nella fisica classica e moderna*
Morris Kline, *La matematica nella cultura occidentale*
Premessa di R. Courant
Alexandre Koyré, *Dal mondo chiuso all'universo infinito*
Seyyed Hossein Nasr, *Scienza e civiltà nell'Islam*
Prefazione di G. de Santillana
Otto E. Neugebauer, *Le scienze esatte nell'Antichità*
In appendice: *Sulla decifrazione delle tavolette astronomiche dei Caldei* di J. Epping
Walter Pagel, *Le idee biologiche di Harvey*
Paolo Rossi, *I filosofi e le macchine 1400/1700*
— *I segni del tempo. Storia della terra e storia delle nazioni da Hooke a Vico*
Silvano Tagliagambe, *Scienza, filosofia, politica in Unione Sovietica (1924/1939)*
Philip P. Wiener, Aaron Noland (a cura di), *Le radici del pensiero scientifico*

Finito di stampare
nel mese di gennaio 1981
dalla Tipolito Milano/Roma
Via Pomezia 10-12, Milano